

*Report of the
Defense Science Board Task Force*

on

DEFENSIVE INFORMATION OPERATIONS

**Volume II- Part 2
Annexes**



June 2001

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

Office of the Undersecretary of Defense
For Acquisition, Technology and Logistics
Washington, D.C. 20301-3140

20010718 091

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2001		3. REPORT TYPE AND DATES COVERED Final Technical, 2001
4. TITLE AND SUBTITLE Defense Science Board Task Force on Defensive Information Operations, Volume II - Part 2 (Protecting the Homeland)			5. FUNDING NUMBERS N/A	
6. AUTHOR(S) Mr. Larry Wright Task Force Chairman				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Science Board Office of the Under Secretary of Defense (AT&L) 3140 Defense Pentagon Room 3D865 Washington DC 20301-3140			8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Science Board Office of the Under Secretary of Defense (AT&L) 3140 Defense Pentagon Room 3D865 Washington DC 20301-3140			10. SPONSORING/MONITORING AGENCY REPORT NUMBER N/A	
11. SUPPLEMENTARY NOTES N/A				
12a. DISTRIBUTION AVAILABILITY STATEMENT Distribution Statement A: Unlimited Distribution			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 words)				
14. SUBJECT TERMS			15. NUMBER OF PAGES 378	
			16. PRICE CODE N/A	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT N/A	20. LIMITATION OF ABSTRACT N/A	

TABLE OF CONTENTS

DSB VOLUME II – DEFENSIVE INFORMATION OPERATIONS PART 2

Annex A – Information Architecture Assurance

Annex B – Technology

Annex C – Organization & Operations

Annex D – Policy

Annex E – Legal

Annex F – 1996 DSB Status Matrix

Annex G – Thought Pieces:

Tab G-1: The Insider Threat & The Low and Slow Attack

Tab G-2: Data/Information/Knowledge/Understanding

Tab G-3: Oversight and Management of the GIG Executive Director

Tab G-4: Red Teaming and the Cyber Operations Readiness Triad (CORT)

Annex H – Reference Data:

Tab H-1: CERT and IO POC List

Tab H-2: Terms of Reference

ANNEX A

**Defense Science Board Task Force
on
Defensive Information Operations**

Panel Report on Information Assurance Architecture

**REPORT OF FINDINGS,
DISCUSSION/OBSERVATIONS
AND RECOMMENDATIONS**

TABLE OF CONTENTS

Executive Summary	1
Chapter 1. Introduction.....	3
Chapter 2. Vision.....	7
Chapter 3. IAA Framework.....	17
3.1 IAA Reference Model	17
3.2 System Architecture	22
3.3 Operational Architecture	28
3.4 Technical Architecture	30
3.5 Metrics.....	33
3.6 Wireless.....	35
3.7 Summary of Findings	35
Chapter 4. "What Might Be Done" Panel Suggestions	41
4.1 The GIG is a Weapon System	41
4.2 Architecture Suggestions.....	44
4.3 Defense in Depth.....	49
4.4 Metric Suggestions	60
4.5 Wireless Suggestions.....	66
4.6 GIG IA Summary	74
Chapter 5. Recommendations.....	77
APPENDIX A. Terms of Reference.....	A-1
APPENDIX B. Bios	B-1
APPENDIX C. Agendas.....	C-1
APPENDIX D. Acronyms.....	D-1

EXECUTIVE SUMMARY

The Information Assurance Architecture (IAA) Panel was tasked to review the implementation of the 1996 Defense Science Board Task Force on Information Warfare Defense recommendations, to identify specific issues associated with information assurance goals of Joint Vision 2020 (JV2020), and to evaluate the adequacy of progress made in achieving these goals. The panel addressed the status of the Department of Defense's (DoD) efforts to establish an IAA framework and standards, and to develop promising IAA techniques. The panel invited representatives from the Services, various agencies, and information technology industries to brief on IA related technologies, trends and market demands. In general, the panel found that significant progress has been made in implementing the 1996 DSB recommendations, but critical issues need to be resolved in the context of JV2020.

The ability to achieve information superiority is the pacing item in realizing the goals of JV2020. The Global Information Grid (GIG) is the underlying infrastructure that will support information superiority. The panel believes the key to success is in implementing a standards-based, metric-driven, end-to-end integrated global information grid. The GIG will incorporate near-term information technologies to globally interconnect information capabilities, associated processes and personnel. Further, the GIG must exploit technologies, standards and architectural frameworks based on commercial information technologies (IT). The panel believes that the implementation of the GIG, in the context of JV2020, is one of those significant events that occur once every decade or two, and that how it is managed and architected will have a major impact on DoD for the next decade or more.

The panel argues that the GIG should be viewed as a weapon system since it leads to information/decision superiority and therefore will be attacked by our adversaries. However, unlike traditional weapons systems, the DoD does not own the critical elements of the GIG; it will be built from rapidly evolving commercial-off-the-shelf (COTS) components. In addition, the GIG can be more readily attacked due to low cost of entry for attackers and the fact that attack attribution is difficult.

The GIG today comprises the Non Secure Internet Protocol Router Network (NIPRNET), Secure Internet Protocol Router Network (SIPRNET), Joint Worldwide Intelligence Communications System (JWICS) and Service Tactical Command, Control, Communications, and Intelligence (C3I) systems. The panel found that each service is pursuing its own architectural implementation of the GIG and observes that, absent an office of primary responsibility, the GIG will not achieve Joint Weapons Systems status. The panel identified a set of DoD strategies for providing information assurance for the GIG: (1) pursue a disciplined implementation through consistent architectural framework; metrics; and commercial standards; (2) segment the communities, i.e., separate DoD from the general public and segment by classification and enclaves; (3) counter denial-of-service by segmentation, redundancy, diversity, and a restricted set of Internet access points; and (4) establish fine grained access control of computing and communication resources.

In addition to developing a strategy, the panel made several assumptions. The first is that the DoD will establish the Internet protocol (IP) as the convergence layer for the GIG. The second is that the Defense Information Infrastructure will migrate from Asynchronous Transfer Mode (ATM) to Internet Protocol (IP) services. The third is that the DoD will fully execute its Public Key Infrastructure/Public Key Enabler (PKI/PKE) strategy.

The panel recommended an Information Assurance (IA) reference model protocol stack that is almost consistent with the reference models used by International Organization of Standardization (ISO) and by the Transmission Control Protocol/Internet Protocol (TCP/IP) community, and is based entirely on commercial protocols. The panel also recommended a standard defense-in-depth approach that spans common user networks, command enclaves, and workstations or servers. It is recommended that all common user networks (SIPRNET, JWICS, and NIPRNET) adopt this approach, which has the feature of providing significant barriers to insider attacks.

The panel observed that the GIG includes commercial as well as DoD wireless connectivity and that the best protection for all wireless systems is at the physical layer. DoD has developed and deployed techniques for such protection; however, commercial wireless systems do not offer equivalent capabilities. Furthermore, both military tactical internets and commercial wireless systems depend on higher-level network processing (routers, user location databases, etc.) that are largely unprotected. Protection needs to be extended to these facilities to ensure robust mobile wireless operations. It will be essential to establish a consistent engineering approach for wireless use in the GIG.

The panel observed that metrics for information assurance are an important and inadequately addressed need. Researchers, designers, vendors and operators of information systems need a broad spectrum of metrics to achieve their respective objectives. The panel observes that it will be necessary to develop different sets of metrics for technical-, systems-, and mission-level evaluation. For instance, mission-level metrics would involve time to complete a mission, targeting and situation awareness accuracy. System-level metrics might include system downtime and response time to neutralize attacks. Technical-level metrics might include probability of attack detection vs. false alarms. The panel also observes that an architectural environment/testbed will be required for development of metrics and measurement of system performance in DoD-relevant operational scenarios and related information traffic flows. To achieve these objectives the testbed must facilitate collaboration and participation of research and development, evaluation and operational communities (services and agencies).

Based on the above, the panel made four principal recommendations: 1) the Secretary of Defense (SecDef) should establish a board of directors to provide oversight of the GIG (Deputy SecDef [Chair], Under Secretary of Defense for Acquisition, Technology & Logistics, VCJS, ASD/CSI, DCI); 2) the Board should establish an Executive Director and systems engineering organization to implement the GIG; 3) the executive director should be given responsibility for implementing the GIG based on a consistent systems architecture; and 4) the executive director should establish a GIG IA research and development (R&D) testbed to meet the need to continually test, evaluate, and evolve the GIG.

By implementing the recommendations and pursuing the layered architectural strategy, vulnerability to attack will be significantly reduced and attribution capabilities will be increased.

CHAPTER 1. INTRODUCTION

Terms of Reference

- Review and assess progress on DSB network security and architecture-specific recommendations associated with information assurance
- Identify network security and architecture-specific issues associated with the information assurance goals of Joint Vision 2020
- Determine the adequacy of progress toward achieving the information assurance goals of JV 2010 on the basis of the network-security-specific requirements
- Develop and submit to the DSB Task Force a summary report

+

Help Develop a Strawman IAA

Figure 1. Terms of Reference

The Information Assurance Architecture (IAA) Panel was asked to review progress made by DoD toward implementing the recommendations made by the Defense Science Board's (DSB) 1996 Study on Information-Warfare-Defense (IW-D).¹ The panel was asked to specifically focus its analysis on those recommendations related to issues associated with DoD information infrastructure architecture initiatives.

At the first meeting of the IAA Panel, the members decided to extend their tasking to include a review of the status of DoD's efforts to establish an IAA framework. The panel felt that such a framework is a necessary foundation for deploying, over time, a DoD information infrastructure that provides a reasonable and understood degree of IA. The panel reviewed the following DoD information-system architectural components: (1) operational architecture (OA), (2) system architecture (SA), and (3) joint technical architecture (JTA). For purposes of IA, the panel added to this triumvirate the need for a reference model for IA – a model that sets a high level perspective of where and how IA services should be provided within the DoD information

¹ Reference 1996 DSB Study "Tactics and Technology for 21st Century Military Superiority"

infrastructure. The need and utility of an IA reference model was predicated upon the fact that such a tool exists and is used in the private sector. We sought to determine if a parallel was developed within DoD as part of its architectural framework for IA. The panel's Terms of Reference (TOR) are provided in Figure 1.

<i>Membership</i>	
▪ Chair:	Dr. Mike Frankel (SRI)
▪ Members:	Dr. Stephen Kent (BBN)
	Dr. Pat Lincoln (SRI)
	Mr. Al McLaughlin (MIT-LL)
	Mr. Peter Steensma (ITT)
	Mr. John Woodward (MITRE)
▪ Government Advisors:	Mr. Lee Hammarstrom
	Dr. Jaynarayan H. Lala (DARPA)

Figure 2. Panel Membership

The members of the IAA Panel who undertook the challenge of addressing the TOR are listed in Figure 2. The members include internationally recognized experts in IA. Their collective expertise included a deep understanding of IA technologies, systems and concepts for both wired and wireless information systems. This understanding included both commercial practices as well as DoD IA implementation and research/development initiatives.

The panel was supported by two government advisors who brought complementary backgrounds and knowledge regarding DoD IA initiatives. One advisor has been a key member of the DoD community architecting, developing, and deploying DoD IA technology for use by DoD Services and Agencies; the second individual brought an understanding of the present DoD IA Science and Technology (S&T) programs.

Brief biographies of the IAA Panel members are provided in Appendix B. Relevant IA backgrounds and experience are noted therein.

Method of Approach

- Review DoD Information Assurance Architecture efforts
- Review commercial IA technology base
- Formulate strawman IAA
 - ❖ Augment DoD efforts
 - or
 - ❖ Start from scratch (not necessary!)
- Identify commercial IA technology shortfalls
- Identify DoD S&T investment strategy
 - ❖ DoD-unique needs
 - ❖ Accelerate private sector efforts
- Define IA metrics

Keep closely coordinated with IA Technology subpanel

Figure 3. Method of Approach

The panel's method of approach for addressing its TOR was to invite DoD representatives from the various organizations supporting DoD IAA programs to brief the panel. Representatives from Office of the Secretary of Defense (OSD), the Services, and Agencies were selected. In addition, representatives from the private-sector information technologies (IT) industry were invited to brief the panel on IA-related technologies, trends, and market demands. Because DoD's information infrastructure, including IA elements, is highly dependent on the private-sector offerings, the panel felt that understanding the needs, goals, and IA architecture frameworks from both perspectives was critical to formulating the panel's findings and recommendations.

Based on this dual track assessment, the panel provided inputs to its companion IA Technology Panel. These inputs were intended to help identify DoD IA requirements for which the private sector would not necessarily provide solutions; thus, a DoD Science and Technology (S&T) investment would be appropriate.

Finally, the panel noted that to measure progress in achieving adequate IA for DoD's information infrastructure, metrics are necessary. At the outset, the panel realized that the definition and development of IA metrics within DoD has only started. The panel, therefore, decided to make IA metrics a key part of its deliberations, as noted in Figure 3.

Meeting Schedule/Planned Topics

2000	Briefings Received	Subject
Feb 22-23	11	Kick-off and IA Service Overviews and Threat Briefings
March 27-28	9	Panel Chairs Outbrief Progress and DoD requirements
April 19-20	15	Joint Vision 2010-2020, DARPA Initiatives, Adequacy of DoD architectures capable of meeting forecasted service and joint requirements
May 24-26	8	DSB Quarterly, DIO Panel briefings to DSB Members. Briefings from Industry and DARPA perspectives.
June 13-14	7	IA metrics, security standards, briefing on Chessmaster.
July 12-13	2	Network information assurance protection measures and Common operating environment. Present findings, develop recommendations and write draft report.
August 7-18	0	DSB Summer Study, final report.

Figure 4. Meeting Schedule

The panel was formed in February 2000 and conducted its business over a period of six months. The first several meetings were dedicated to receiving briefings and the latter to panel discussions and formulation of the findings and recommendations provided in this report.

As noted in Figure 4, a total of 52 briefings were received covering the topics and organizations noted therein. The major themes for each of the six meetings held are also noted in the figure. The specific briefings and briefers presented are provided in Appendix C.

The briefings and the backgrounds of the panel members provided the contextual and technical information that formed the basis of the findings and recommendations provided herein.

CHAPTER 2. VISION

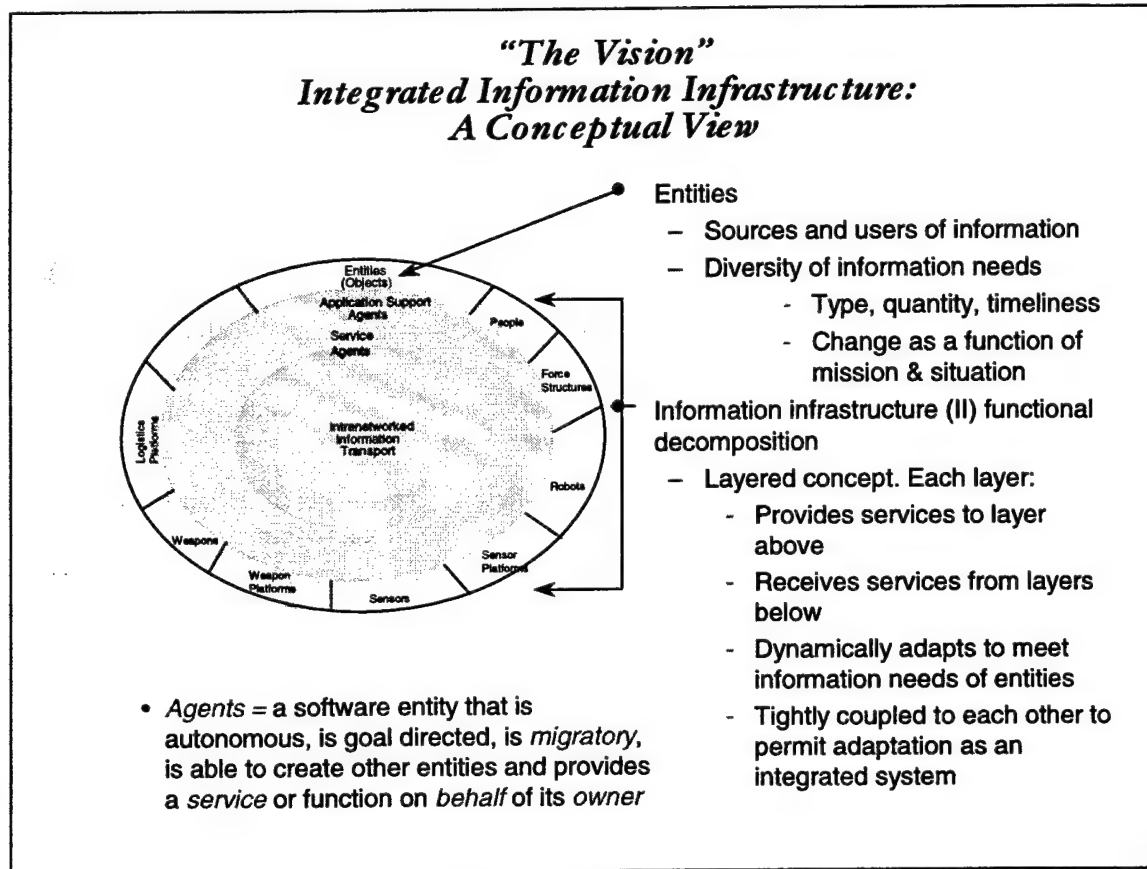


Figure 5. III Vision

In prior DSB studies, a vision, called the Integrated Information Infrastructure (III), was developed for DoD². This vision, as discussed below, has become the foundation within DoD for many of its information infrastructure initiatives today. The vision sets goals and directions for DoD-wide information services that will come about through the exploitation of private sector information technology (IT), to include associated IA technologies. The III then sets both a long-term vision and a road map for the evolution of the DoD infrastructure. Figure 5 provides a conceptual view of the III.

The ability to achieve information superiority is the pacing item in realizing the goals of Joint Vision 2020. The inadequacies of current service information infrastructures prevent commanders from realizing the full benefit of the current family of intelligence, surveillance, and reconnaissance (ISR) systems – space-based, airborne, or surface – much less profiting from advances in sensors and weapons. Because of uncertainties whether crucial information will be available when needed, commanders are driven to develop unique, local-only reconnaissance,

² Reference 1996 DSB Study "Tactics and Technology for 21st Century Military Superiority"; 1998 DSB Summer Study "Joint Operations Superiority in the 21st Century"; 1999 DSB Summer Study "21st Century Defense Technology Strategies"

surveillance, and target acquisitions (RSTA) systems. Overall, this tendency has resulted in redundant investment in, and proliferation of, "stovepipe"³ communication and sensor systems.

Increasingly, the armed forces are shifting to an operational concept wherein surveillance and targeting sensors are separated physically from the command node location, which in turn may be remote from the weapons launch platform. In the case of air platforms, for example, no longer will the sensors, commander (pilot), and weapons necessarily be collocated in a single aircraft. Further, third party targeting data sources and weapons magazines are proliferating. Examples of this evolving trend appear in such concepts as forward pass, cooperative engagement capabilities (CEC), the arsenal ship, and the transfer of tactical situation data derived from a variety of off-board sources directly into cockpits.

This evolution promises major improvements in the tactical flexibility and combat effectiveness of forces. The realization of this promise is not without challenges, however, because the operational concept is inhibited by the inadequacy of the traditional military communication and information-services infrastructure as well as continuing interoperability problems between military services and between systems within a given service.

To realize the potential benefit of this new concept, our future information infrastructure must be capable of reliable transmission, storage, retrieval and management of large amounts of data. Today all systems are segmented into communications links, computers, and sensors that in turn are stovepiped to support specific functions (i.e., intelligence, logistics, and fire control). Furthermore, these component entities are now constrained by a lack of (1) the bandwidth necessary for high-resolution imagery transfer; (2) the processor capacity needed for target recognition and interpretation; (3) memory sufficient to handle massive amounts of archival data; and (4) software to search the many data repositories quickly in order to provide commanders with tactical information in a timely manner. These constraints are magnified by difficulties in integrating a myriad of legacy information systems with newly developed, service-unique stovepipe and joint systems. These limitations can be overcome, and the full capability of joint forces realized, if we set as our goal the integration of all military C4ISR⁴ systems into a ubiquitous, flexible, interoperable C4ISR system of systems – the Integrated Information Infrastructure.

The Integrated Information Infrastructure must meet several key requirements if it is to enable future combat operations to support a wide spectrum of missions, threats, and environments.

As stated in Joint Vision 2020, a military force must be able to receive or transmit all of the information it needs for the successful and efficient prosecution of its mission, from any point on the globe, in a flexible, adaptive, reconfigurable structure capable of rapidly adapting to changing operational and tactical environments. The information infrastructure must support this need, while allowing force structures of arbitrary composition to be rapidly formed and fielded. Furthermore, the infrastructure must adapt to unanticipated demands during crises, and to stress imposed by adversaries.

³ "Stovepipe" systems are those designed with one application or uses in mind without consideration of interfaces with other systems.

⁴ C4ISR: Command, control, communications, computers, and intelligence surveillance and reconnaissance.

The infrastructure must allow information to be distributed to and from any source or user of information at any time: its architecture must not be constrained to support a force-structure (enterprise) hierarchy conceived *a priori*. Most importantly, the information and services provided to an end user through the infrastructure *must be tailored to the user's needs, and be relevant to the user's mission, without requiring the user to sort through volumes of data or images.*

The information infrastructure must include multimode data transport including landline, radio, and space-based elements. All of these media must be integrated into a ubiquitous, store-and-forward data internetwork that dynamically routes information from source(s) to destination(s), transparently to the user. This data transport segment of the infrastructure must be self-managed, be adaptive to node or link failure, and provide services to its users based on quality-of-service (QoS) requests. These services include bandwidth, latency, reliability, precedence, distribution mechanisms (point to point, point to multipoint), and the like.

The infrastructure interface will link the user to a distributed processing environment that includes all types of computers situated at locations appropriate to their needs for power, environment, and space. This distributed computing environment will be integrated via the transport component of the infrastructure, thus enabling these processors to exchange data dynamically, share computation loads, and cooperatively process information on behalf of and transparent to the user.

The infrastructure should be an adaptive entity that integrates communication systems, computers, and information management resources into an intelligent system of systems. Each component of the III will exchange state information with each other, in order to enable the entire infrastructure to adapt to user requirements and any stresses imposed on the network by an adversary. This adaptability will also enable the infrastructure to change its scale as necessary to support force structure(s) of arbitrary size, or to incorporate new processing, network, and communication technologies as they are developed. Thus, this infrastructure is a scaleable computing environment.

The information infrastructure must provide tailored information services to diverse users ranging from a single person to a collection of people, sensors, and/or weapons by means of intelligent agents – software entities, under the general control of the user, that are goal-directed, migratory, and able to create other software entities, and provide services or functions on behalf of the user.

Each user will be served by one or more intelligent software agents that *proactively* provide and disseminate appropriately packaged information. These agents will perform such functions as fusing and filtering information and delivering *the right information to the right user at the right time*. They must be proactive in the sense that they are aware of the user's situation and needs, and can provide information relevant to those needs without a specific user request.

These agents will multiply the personnel resources available to combat units by gathering and transforming data into actionable information to support unit operations, just as unit members would have to do, were the software agents not provided. Warfighters will therefore be freed of routine chores in favor of actual operations.

To the maximum extent feasible, the infrastructure's transport layer will take advantage of commercial technology and networks, by utilizing open-systems standards and protocols, and will minimize the use of service- or function-unique hardware and software. For applications where military-unique capabilities (such as antijam, low probability of intercept, spread-spectrum waveforms and the like) are required, military products will be developed or adapted to interface with the overall architecture.

We must set as a goal the realization of the III vision in an evolutionary manner. As we succeed, we will enable, over time, the following military capabilities:

- Geographic separation and functional integration of command, targeting, weapons delivery, and support functions
- Support for split-base operations, force projection, information reach back, combat, and force protection for units large and small
- Common situational understanding, common operating picture, and informed and rapid decision making for joint forces
- Enhanced operational flexibility for commanders at all levels
- Reduced logistics footprints in immediate combat areas
- Full exploitation of sensor, weapon, platform and processing capabilities
- Real-time or near real-time responsiveness to commanders' requests for information, fire support, and urgent logistics support

The first phase for realizing the III is the implementation of the Global Information Grid (GIG). The GIG will incorporate near-term information technologies to provide the warfighting capabilities noted above. The GIG will, over time, evolve into the longer-term vision for the III. As we proceed to implement and secure the GIG, we must keep the evolution toward the III in mind.

Global Information Grid (GIG)

Definition

Globally interconnected, information capabilities associated processes and personnel for
collecting processing
storing disseminating
managing information
on demand to warfighters, policy makers, and supporters

The GIG includes:
all owned and leased communications
computing systems and services
Software, applications and data
security services

The GIG supports:
Department of Defense
National Security activities
Intelligence community
missions in war and in peace

The GIG provides capabilities from all operating locations:
bases posts camps stations
facilities mobile platforms deployed sites

The GIG provides interfaces to coalition, allied, and non-DoD users and systems

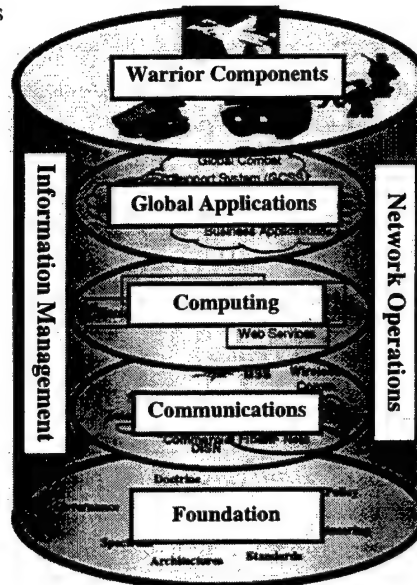


Figure 6. Global Information Grid

The III vision was formulated in 1996. It, along with similar visions such as Network Centric Warfare (NCW) and the Advanced Battlefield Information System (ABIS), has helped DoD formulate and articulate a vision for a near-term version of the III. This near-term vision is shown in Figure 6. The GIG is intended to be the means by which information superiority (IS), as envisioned in the Joint Vision 2020, is achieved. The following quotes define the GIG.

The GIG is the vision of the Assistant Secretary of Defense for Command, Control, Communications, Computers, and Intelligence (ASD/C3I) for achieving IS. The GIG is focused on the warfighters' needs for IS plus the critical concerns of frequency spectrum and improving the management of the information infrastructure investment along with the coevolution of Doctrine, Organization, Training and Education, Materiel, Leadership, Personnel, and Facilities (DOTMLPF).⁵

The September 22, 1999, Office of the Assistant Secretary of Defense Director, Command, Control Communications and Intelligence Systems (ASD/C3I) memorandum, Subj: Global Information Grid, defines the Global Information Grid (GIG) as:

⁵ Reference: *Enabling the Joint Vision*, The Joint Staff, C4 Systems Directorate, Information Superiority Division (J6Q), Pentagon, Washington, D.C., March 2000

The globally interconnected, end-to-end set information capabilities, associated processes and personnel for collecting, processing, sorting, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operations locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). GIG provides interfaces to coalition, allied, and non-DoD users and systems.

The GIG's interoperability builds upon the existing Defense Information Infrastructure (DII) Common Operating Environment (DII-COE). The building blocks of Joint Technical Architecture, Joint Operational Architecture, Joint Systems Architecture, a shared data environment, the migration of legacy systems, and adherence to commercial standards provide the necessary structure for the GIG.

The key to achieving information superiority lies in implementing a standards based, metric-oriented, end-to-end integrated Global Information Grid. The concept of IS may be situational but the GIG, which will implement IS, is quantifiable. Important initiatives to implement the GIG are described in the following sections.

The emphasis on the standards-based and metrics-oriented aspect of the GIG description is believed by the panel to be key to its being successfully deployed, used and evolved to continuously meet DoD needs.

Integrated Information Infrastructure Roadmap

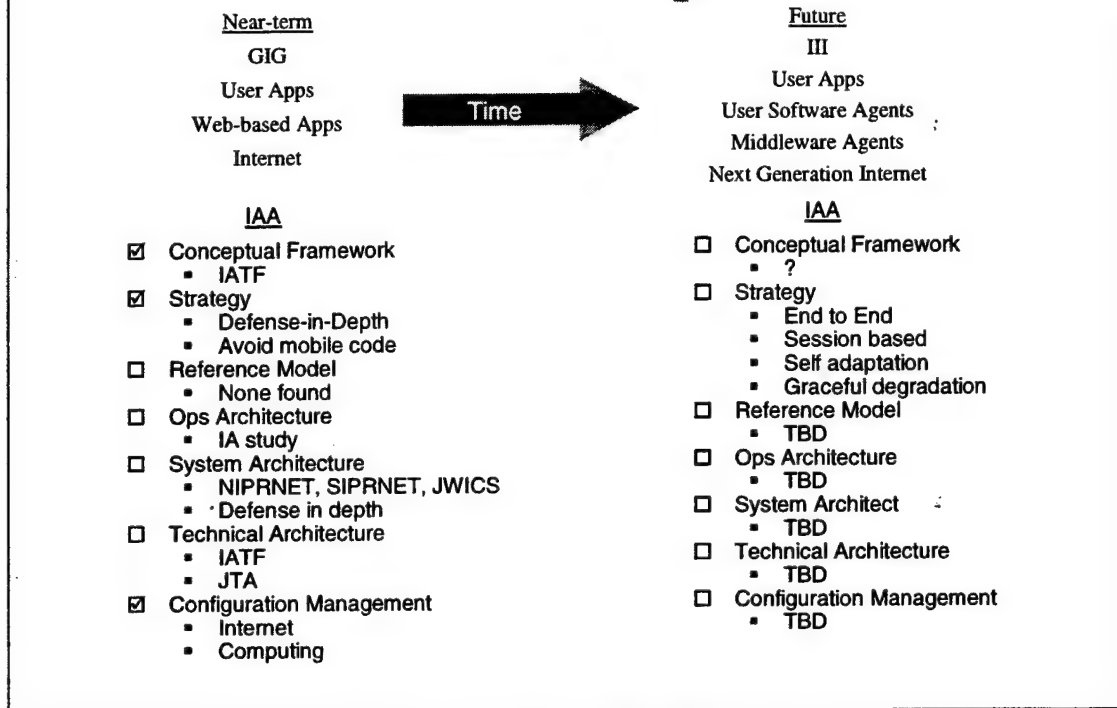


Figure 7. III Roadmap

The evolution of today's GIG into the III envisioned by the DSB requires that the GIG exploit technologies, standards and architectural frameworks based on information technologies (IT). It is within the private sector that significant investment in and rapid evolution of IT is occurring. DoD must position its evolving GIG to take advantage of this technological evolution.

Figure 7 shows the evolution of the GIG. As noted, its foundation architectural framework must be sufficiently flexible to allow transition from more conventional relational/procedural-based information services to services supported by intelligent mobile code (software agents). Keeping this evolution in focus today will help DoD augment the GIG when necessary as well as help to guide DoD's science and technology (S&T) investments over the next several years.

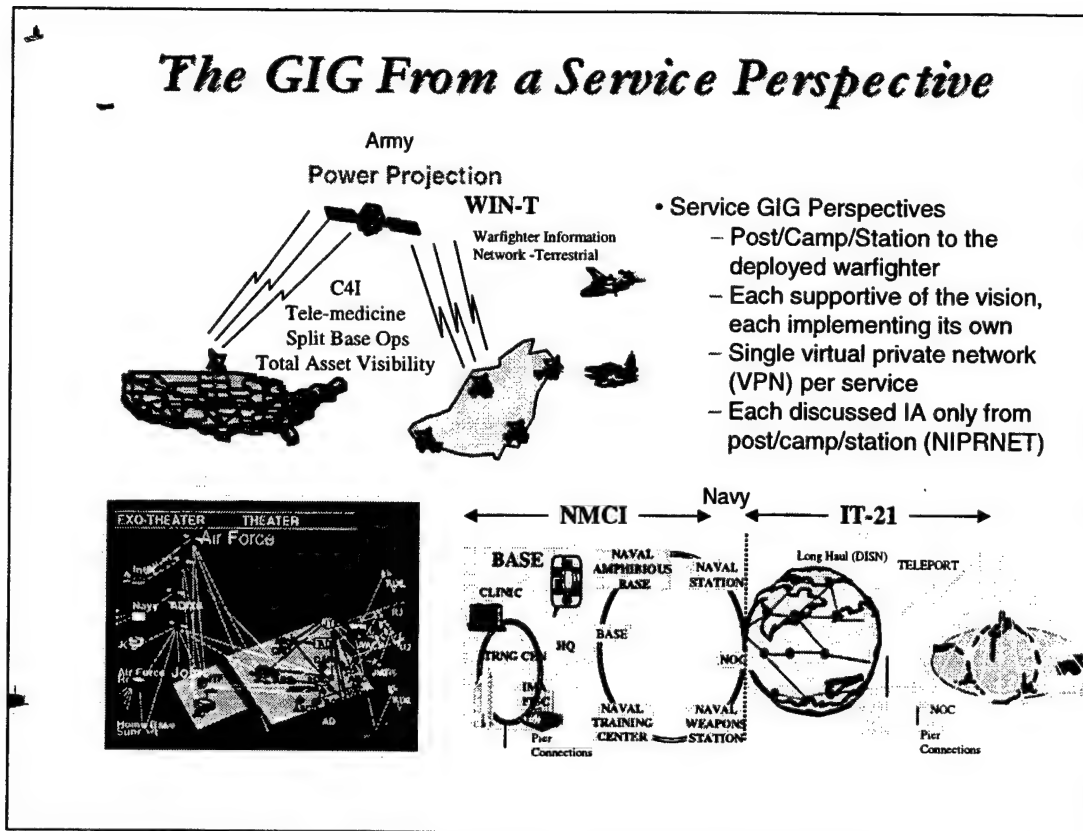


Figure 8. The GIG from a Service Perspective

In addition to hearing the OSD perspective, plans, and strategy for the GIG, the panel heard the service views on GIG. In each case, as shown in Figure 8, the Services presented an overview of the GIG that was consistent with the notion of an integrated infrastructure connecting post, camp, or station to deployed forces. The infrastructure, from each service's perspective, would support warfighter applications, combat service functions, and business functions for each of its user communities wherever they are situated.

The panel noted, though, that each service presented and talked to *its* implementation of a global information grid – none presented a concept of a single, joint, DoD-wide GIG which would be leveraged and used for its information needs. The panel did not hear how the services' need for various levels of security (unclassified through top secret) would be supported in their respective implementations. In fact, the panel noted that the primary focus of the Services' presentations was supporting post/camp/station unclassified information services. The panel also heard that each service anticipated having wireless access media integrated into its respective segment of the GIG. This wireless media is necessary to support our highly mobile, forward-deployed forces. In addition, the panel noted that wireless point-to-point extensions exist in the "wire-based" (fiber or copper) segments of the GIG that support the interconnection of the post/camp/station locations. These wireless media need to be considered when one addresses IAA for the GIG. This issue, not discussed in DoD briefings, is addressed more fully in subsequent sections of this report.

Panel Findings

An amazing amount of *progress has been made* during the past year in formulating an IAA strategy, framework, associated architectures and implementation of infrastructure

“people, resources, technology

+

the IATF* “reference manual”

But:

Additional work remains

* Information Assurance Technical Framework

Figure 9. Panel Findings

From the DoD and service-related briefings, the panel noted that significant progress has been made in formulating an IAA strategy, framework, and associated architecture and in implementing infrastructure. The IAA Panel noted that significant people, funds and technology have been allocated and deployed toward providing a more robust DoD information infrastructure. This section of our report presents the panel’s findings related to this progress.

CHAPTER 3. IAA FRAMEWORK

3.1 IAA REFERENCE MODEL

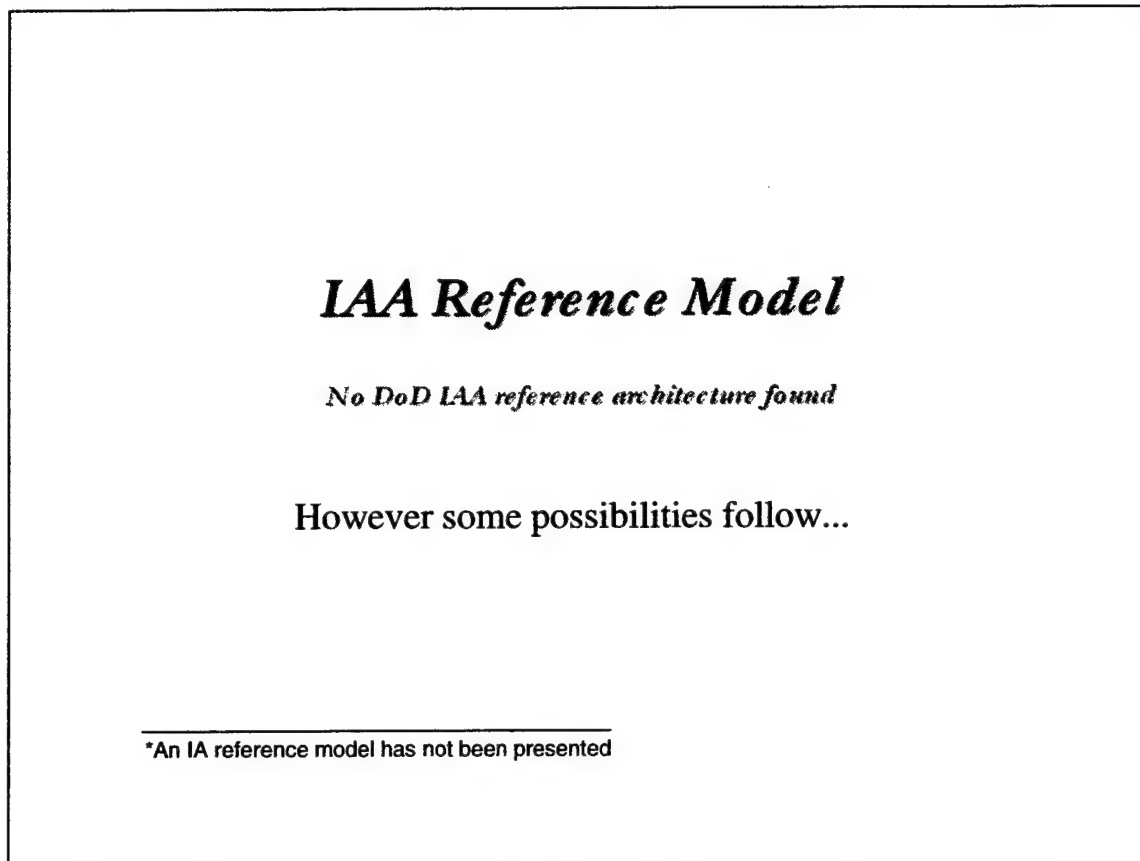


Figure 10. IAA Reference Model

As shown in Figure 10, no single IAA reference model (RM) has been selected or developed by DoD. Such a reference model would help the DoD IA community understand where appropriate IA standards and services are provided within the GIG. Given that a RM has not been selected, the panel noted that various options do exist.

ISO Reference Model & Security Protocols

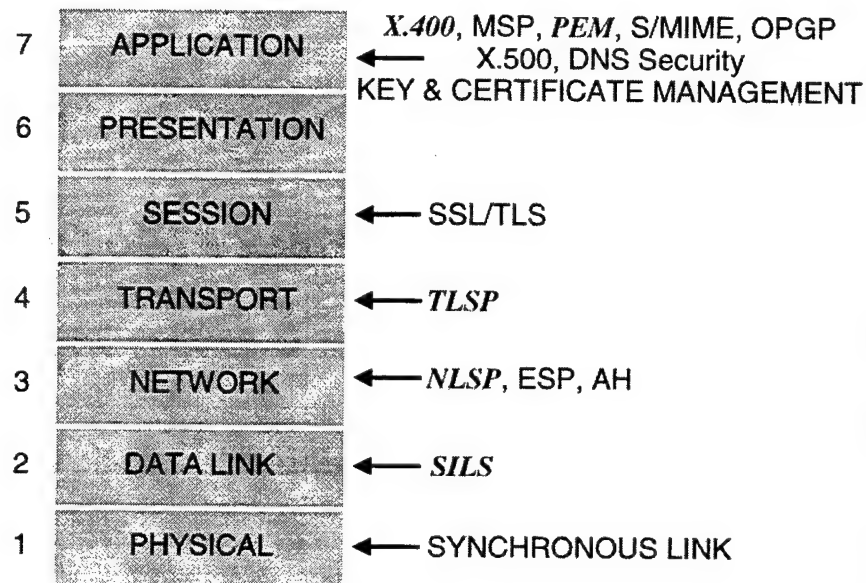


Figure 11. ISO Reference Model and Security Protocols

Figure 11 presents one option. This figure illustrates the International Organization of Standardization (ISO) reference model (ISO 7498) annotated with a mix of International Telecommunications Union (ITU-T) (see ISO and Consultative Committee on International Telegraph and Telephone [CCITT]) and Internet Engineering Task Force (IETF) security protocol standards. (The term “synchronous link encryption” is non-standard and refers to physical layer cryptographic devices employed on a per-link basis. The term “key and certificate management protocols” is also non-standard.) The standards highlighted in *italics* are obsolete, either superseded by newer standards or never adopted by vendors and integrated into products.

The protocols noted in Figure 11 include:

- Standard for Interoperable LAN Security (SILS), Institute of Electrical and Electronics Engineers (IEEE) 802.10
- Network Layer Security Protocol (NLSP), an ISO protocol
- Encapsulating Security Payload (ESP) and Authentication Header (AH), Internet Engineering Task Force (IETF) protocols defined in RFCs 2402 and 2406
- Transport Layer Security Protocol (TLSP), an ISO protocol

- Secure Sockets Layer (SSL)/ Transport Layer Security (TLS); the former is a commercial security protocol, the latter is the IETF version
- X.400, Message Security Protocol (MSP), Privacy Enhanced Mail (PEM) Secure MIME (S/MIME) and Open PGP (OPGP), all are secure e-mail protocols. X.400 is a CCITT standard, MSP is a DoD standard, and PEM, S/MIME and OPGP are IETF standards
- X.500 and DNS Security are directory security standards from the CCITT and IETF, respectively

ISO Reference Model: Mapping Services to Protocol Layers

Layers

Service	1	2	3	4	5	6	7
Peer Entity Authentication	•	•	Y	Y	•	•	Y
Data Origin Authentication	•	?	Y	Y	•	•	Y
Access Control Services	•	?	Y	Y	•	•	Y
Connection Confidentiality	Y	Y	Y	Y	•	•	Y
Connectionless Confidentiality	•	Y	Y	Y	•	•	Y
Selective Field Confidentiality	•	•	•	•	•	Y	Y
Traffic Flow Confidentiality	Y	•	Y	•	•	•	Y
Connectionless Integrity	•	?	Y	Y	•	•	Y
Selective Field Integrity	•	•	•	•	•	•	Y
Non-repudiation, Origin	•	•	•	•	•	•	Y
Non-repudiation, Receipt	•	•	•	•	•	•	Y

Figure 12. ISO Reference Model

Figure 12 illustrates the mapping of security services (as defined in ISO 7498-2) to the seven layers of the ISO reference model shown in Figure 11. It is extracted from a more comprehensive larger table in ISO 7498-2. The table is intended as a guide for protocol developers, suggesting which security services may be appropriate to offer at which layers. Even without examining each cell in detail, several issues are apparent. The question marks at layer 2 represent a disagreement between ISO and IEEE, which was eventually resolved in favor of the IEEE (re SILS). Layers 3 & 4 offer similar security features. No security services are recommended for the

session layer (5), and little is appropriate for layer 6. Any security service can be offered at layer 7.

Note that the same service may be offered at multiple layers without being redundant, because different layers provide different communication services. So, for example, excellent traffic flow confidentiality can be offered at layer 1, but end-to-end confidentiality requires use of layer 3, 4 or 7.

In the IA reference model recommended by the panel, we propose adoption of standard security protocols at layers 3, 5, and 7. We also emphasize the use of layer 1 (physical layer) security technology (i.e., link encryption or Transmission Security [TRANSEC] for wireless links) to connect DoD network elements.

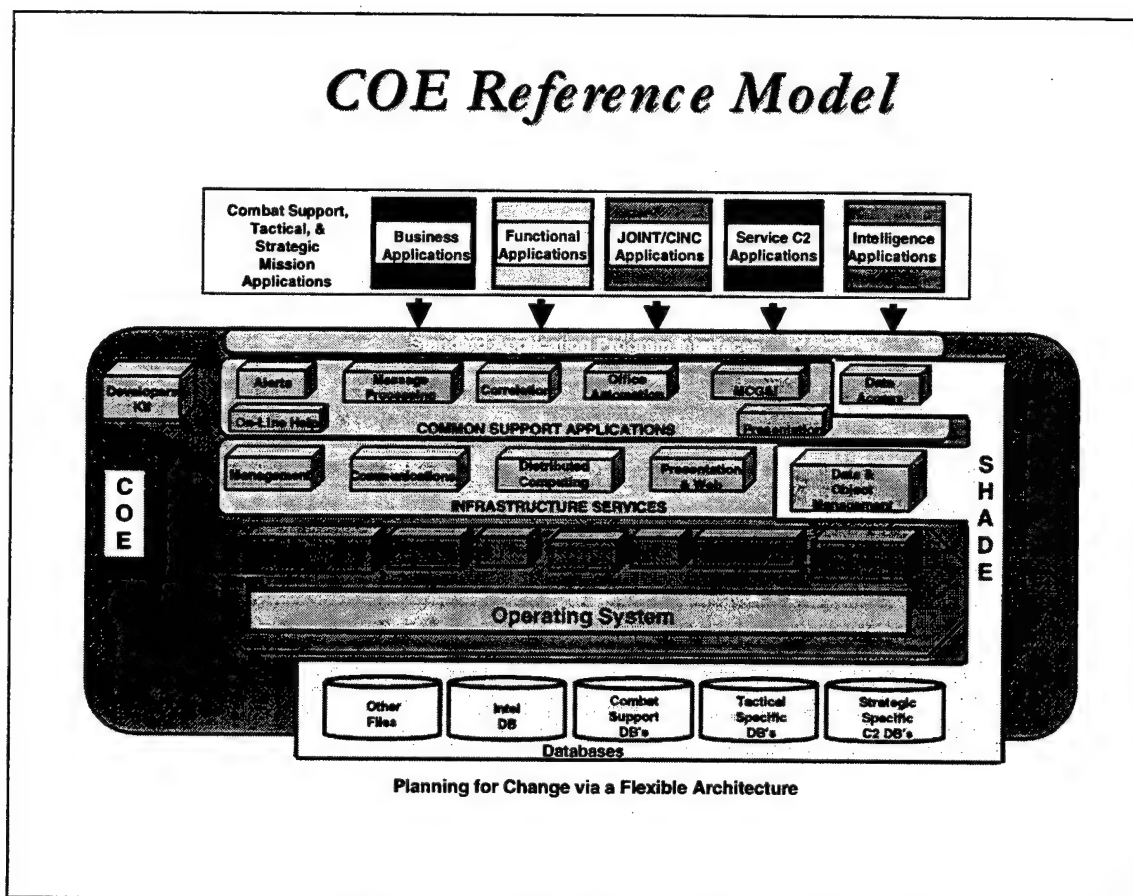


Figure 13. COE Reference Model

A second option for a GIG RM is extending the Common Operating Environment RM (COE) shown in Figure 13. This reference model illustrates the segmentation and layering of code and services in the COE. The panel noted, however, that the COE does not yet address IA (security) services within either its RM or within the run time environments or segmented code libraries it provides to DoD customers. Through discussions with DoD COE representatives, the panel learned that IA extensions to the COE RM, to identify IA services, are presently underway, but there are no near-term plans to add IA (security) code to the COE run time environments. The

panel also noted that the COE is a product-centric framework as opposed to a standards-centric framework that is one of the underlying tenets of the GIG (see discussion in Figure 6).

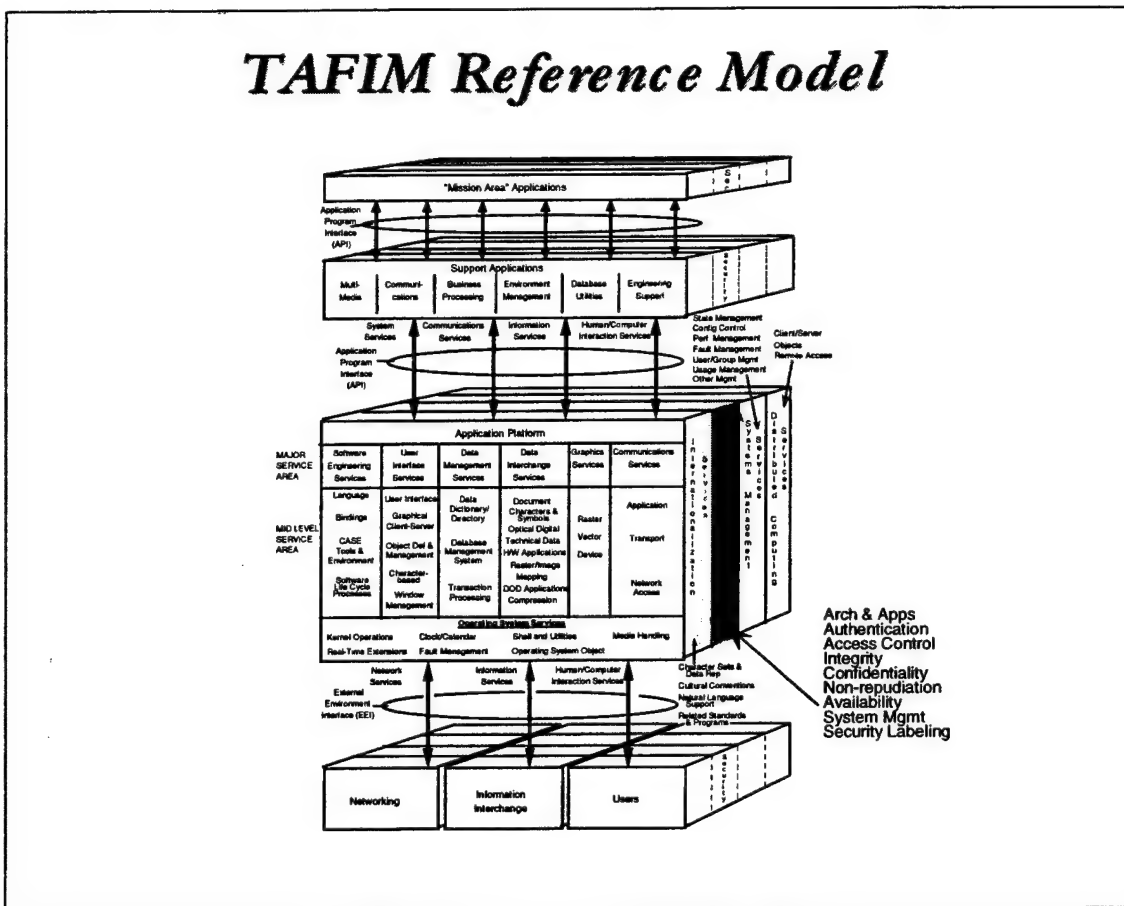


Figure 14. TAFIM Reference Model

A third possible IA reference model is shown in Figure 14. This model comes from an earlier DoD initiative to establish a vision and framework for information systems and services within the Department. This earlier effort, called the Technical Architecture for Information Management (TAFIM), attempted to compile industry and DoD standards, practices and architectures associated with enterprise-scale, distributed, information systems. In this reference model, security services are identified as a backplane of the application platform. The security services provided to the "mission-area" applications include: authentication, access control, integrity, non-repudiation, availability, system management, and security labeling.

The TAFIM RM did not provide sufficient information to allow system implementers to select a specific set of protocols to provide IA services for their users. Because of its lack of specificity the TAFIM has been replaced with more current and focused technical guidance documents (i.e., the Joint Technical Architecture – [JTA]) and run time environments (i.e., the COE).

Of the three possible IA RMs presented, the panel suggests that DoD select the Open Systems Interconnect (OSI) framework. In the section of this report entitled "what can be done," (see Section 4) the rationale for this suggestion is presented.

3.2 SYSTEM ARCHITECTURE

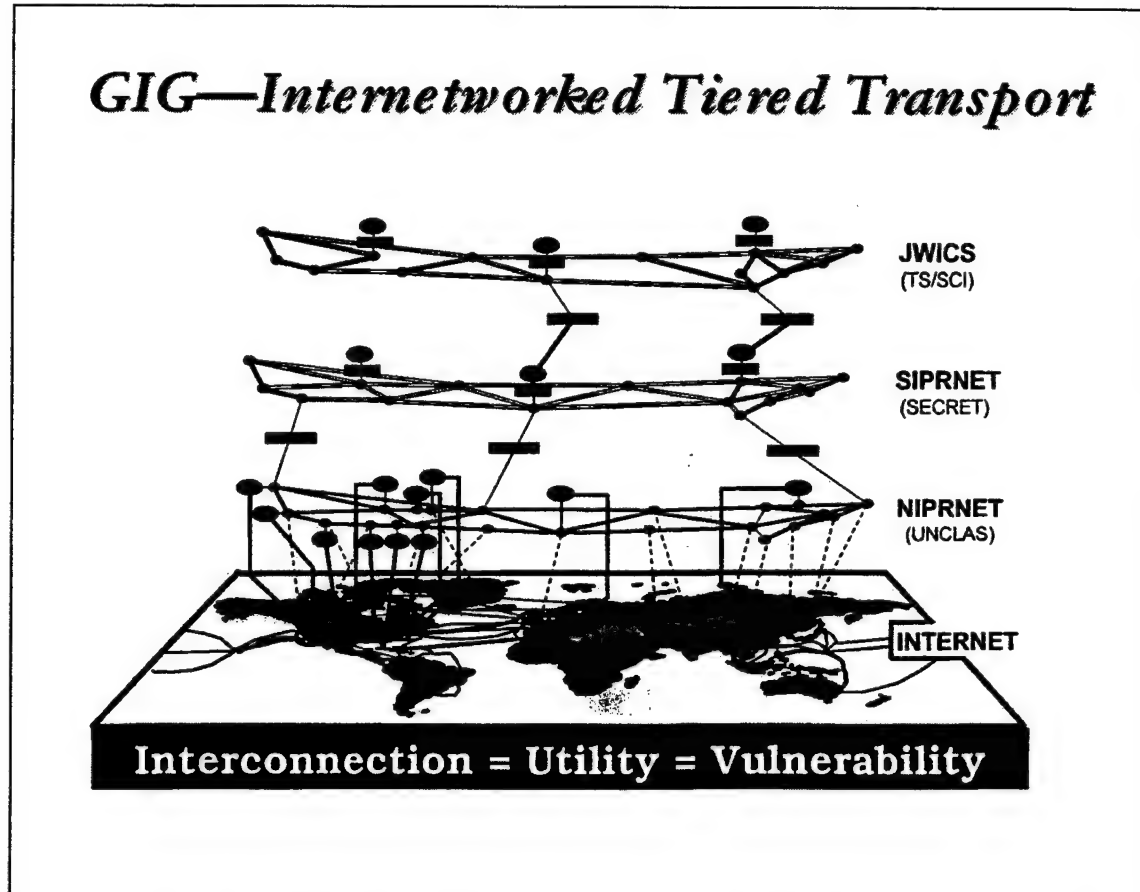


Figure 15. GIG—Internetworked Tiered Transport

As shown in Figure 15, the system architecture for the telecommunications component of the GIG, as it exists today, comprises three virtual, worldwide data networks. These networks include the non-secure Internet Protocol (IP) network (NIPRNET), the secret IP network (SIPRNET), and the Joint World-Wide Intelligence Communication System (JWICS). The NIPRNET, which supports unclassified (but possibly sensitive) DoD data communications, has been part of the private sector World Wide Web (WWW). It is accessible, in principle, by all WWW users and is connected to the packet-switched routing infrastructure (the public Internet) that underlies the WWW. Interconnection points between DoD NIPRNET systems (host, routers, and access points) and the public Internet have been many hundred and mostly unmanaged by DoD.

Recently, DoD has decided to limit these access points to 8 to 11 monitored gateways between a virtual NIPRNET and the public Internet. Additional connection points could be allowed but are planned, at present, to be few in number and carefully controlled by DoD.

The SIPRNET is a secret-high virtual private DoD network. This system uses encrypted links between the routers that connect user sites, to secure transmission of secret data. User sites, and their corresponding competing resources, are all run at secret high. The panel notes that the SIPRNET traffic can (and probably does) transit the same physical transmission links (fiber, copper, and wireless systems) as does NIPRNET traffic – the former being encrypted, the latter being transferred primarily in the clear.

JWICS is also a virtual private network supporting the exchange of Top Secret (TS), Sensitive Compartmented Information (SCI) between user sites. JWICS, similar to SIPRNET, appropriately encrypts information for transmission over the communication links that connect the routers at each user site and transfers this data across the same commercial (and government-owned) transmission facilities used by the NIPRNET. Thus, JWICS, SIPRNET, and NIPRNET are cryptographically segmented virtual private networks (VPNs) that likely share common physical communication media. In the current system, these VPNs are implemented at the physical layer, which offers good security in many respects. Somewhat different features arise if one also creates VPNs at the IP layer, as we discuss later.

The panel was also informed that traffic can flow between JWICS and SIPRNET and between SIPRNET and the NIPRNET via trusted guards. These guards automatically filter the type and quantity of data that flows between these virtual networks. Their use is a risk/benefits tradeoff that has placed user and enterprise value on allowing limited traffic flow of appropriately sanitized information between virtual networks of different classification levels while accepting the risk of having unfiltered information pass the network boundaries or possibly opening covert channels of information flow from the classified to the unclassified communities (possibly by virtue of an insider threat).

Another key aspect of the system architecture suggested by Figure 15 is that all DoD general information resources are on the NIPRNET. Thus, private sector users needing access to this general, public information are required to gain access to the DoD computer servers storing this information. Although DoD has had issues with hackers and malicious entities trying to deface or gain access to their Web sites, the present plan is still to filter access to these sites – yet everyone must still be granted access to this general information at many DoD sites maintaining this information. The DoD is aggressively deploying a defense-in-depth strategy, as discussed in the next figure, but it must still provide and support access to all NIPRNET DoD sites for the general public and those elements of the private sector with which DoD conducts e-commerce. This planned approach makes it harder to design and deploy an effective defense-in-depth approach.

The panel also noted that the GIG is really, today, the aggregation of the JWICS, SIPRNET and NIPRNET virtual private networks. These networks, together, constitute the starting point for the GIG. Consequently, one should think of the SIPRNET as the VPN that provides (secret level) secure data/information transfer from post/camp/station to the “foxhole.” Thus, all service secret-level combat mission functions and their supporting computers and communications should be viewed as being integrated into the SIPRNET. Similarly, the NIPRNET VPN should be viewed as the network supporting unclassified but sensitive (UBS) combat information services such as in-the-field logistics and medical and troop deployment/movement. If this perspective is taken, a means of more fully protecting the NIPRNET is required. A suggested architecture will be provided in the section of this report entitled “What Might Be.”

Finally, the panel notes that both the SIPRNET and JWICS provide virtually no protection against the insider threat. This issue is also addressed Chapter 4 entitled “What Might Be Done” later in this report.

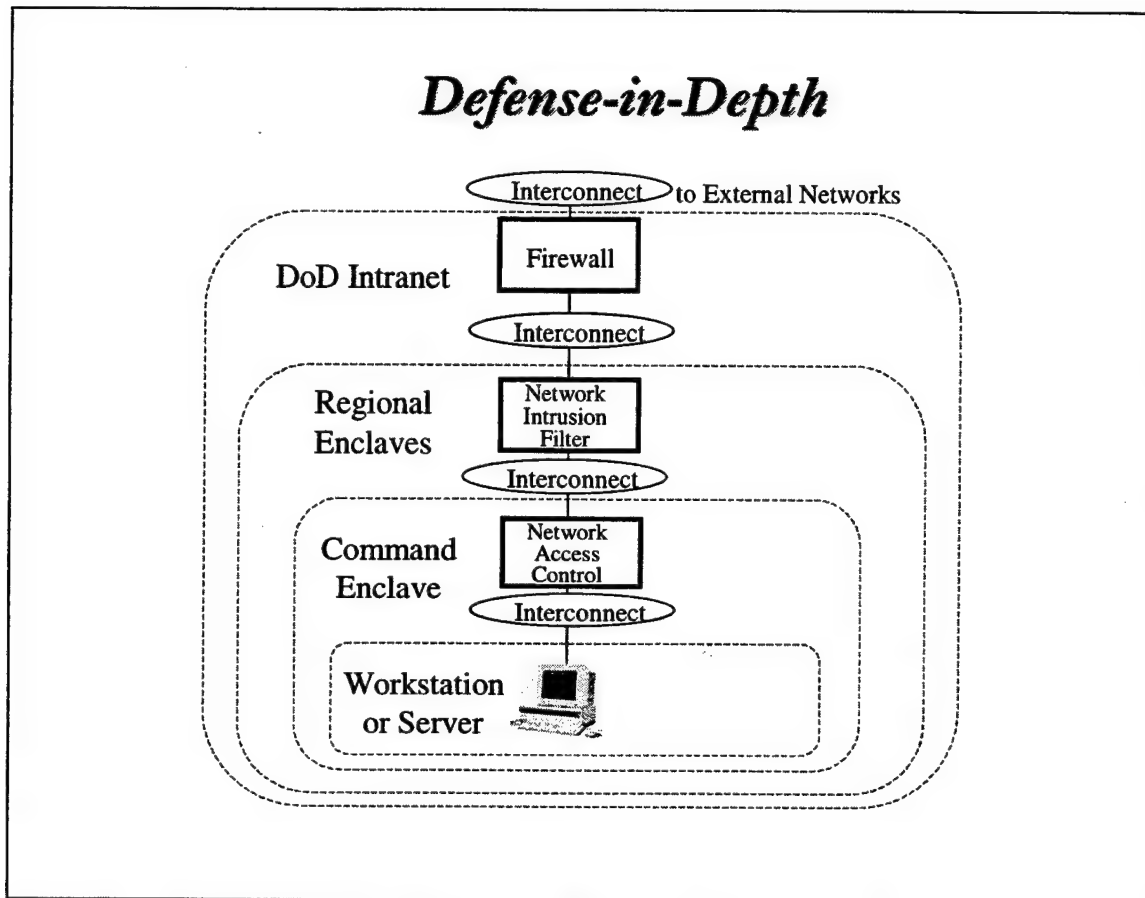


Figure 16. Defense-in-Depth

Figure 16 shows the “defense-in-depth” (DiD) strategy DoD is employing to try to protect its publicly accessed sites on the NIPRNET. The basic concept of defense-in-depth is to provide multiple layers of security mechanisms between computing elements (workstations and servers) in a particular enclave and computing elements in other enclaves, the DoD Intranet, or external networks. There are four focus areas of defense-in-depth: defend the computing environment; defend the enclave boundary; defend the network; and establish supporting infrastructures. Defending the computing environment includes properly configuring operating systems and application software, along with using host-based security services such as anti-virus software, intrusion detection, and public key cryptography. Defending the enclave boundary includes identifying all enclave boundaries, employing firewalls at these boundaries, and detecting intrusion at the enclave-level. Defending the network includes using link encryption for classified networks, firewalls, and intrusion detection. Supporting infrastructures include PKI (public key infrastructure) services and services that support network management, intrusion detection, and intrusion response.

Army IAA System Deployment

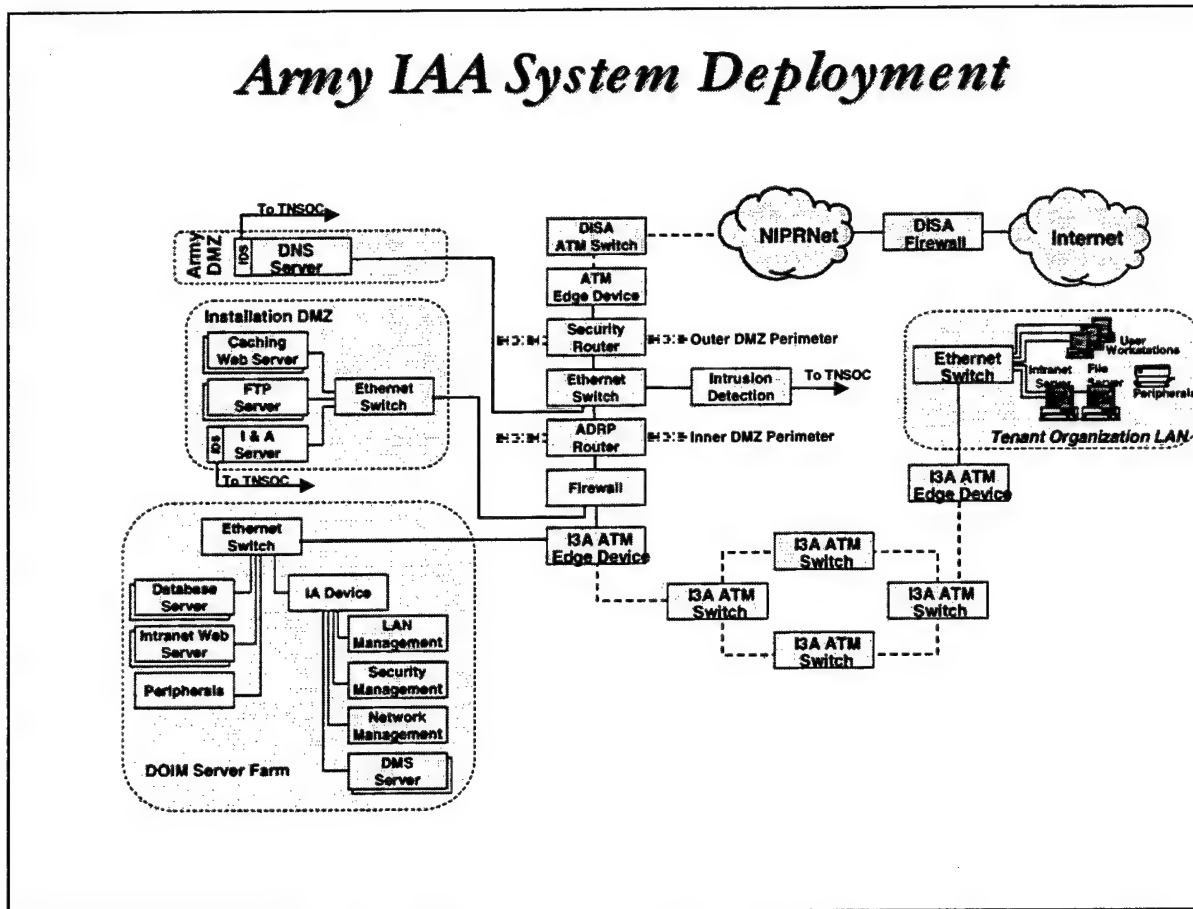


Figure 17. Army IAA System Deployment

The Army is applying a defense-in-depth (DiD) strategy to their NIPRNET post/camp/station enclaves as shown in Figure 17. In this particular system architecture, the Army is accepting that Defense Information Systems Agency (DISA) is providing asynchronous transfer mode (ATM) services to the enclave boundary. A router then provides a translation from the native ATM backbone to an IP-based network interface in the demilitarized zone (DMZ) and to an Ethernet interface within the enclave itself.

In the Army's implementation of DiD, the Army's public information servers are within the installations DMZ. All access from the WWW (public use) comes from the Internet through the NIPRNET, to the installation perimeter, then through the ATM switch, perimeter IP router and an Ethernet switch (at which point intrusion detection is conducted) to the installation servers. Thus *all* public users are funneled to the installation's DMZ for general information services.

In this implementation, there is then an additional IP router, a firewall and an ATM switch to convert from IP back to native ATM. These are then the backbone for the installation server farm and tenant organization's local area networks (LANs). This multiple conversion from ATM to IP to Ethernet to IP to ATM can cause latency and throughput problems (due to multiple protocol translations). This system architecture does provide the opportunity to use higher bandwidth (relative to existing IP network encryptors) ATM network encryptors where necessary. There

does appear to be uncertainty, however, as to why this multiple protocol translation is necessary or desirable.

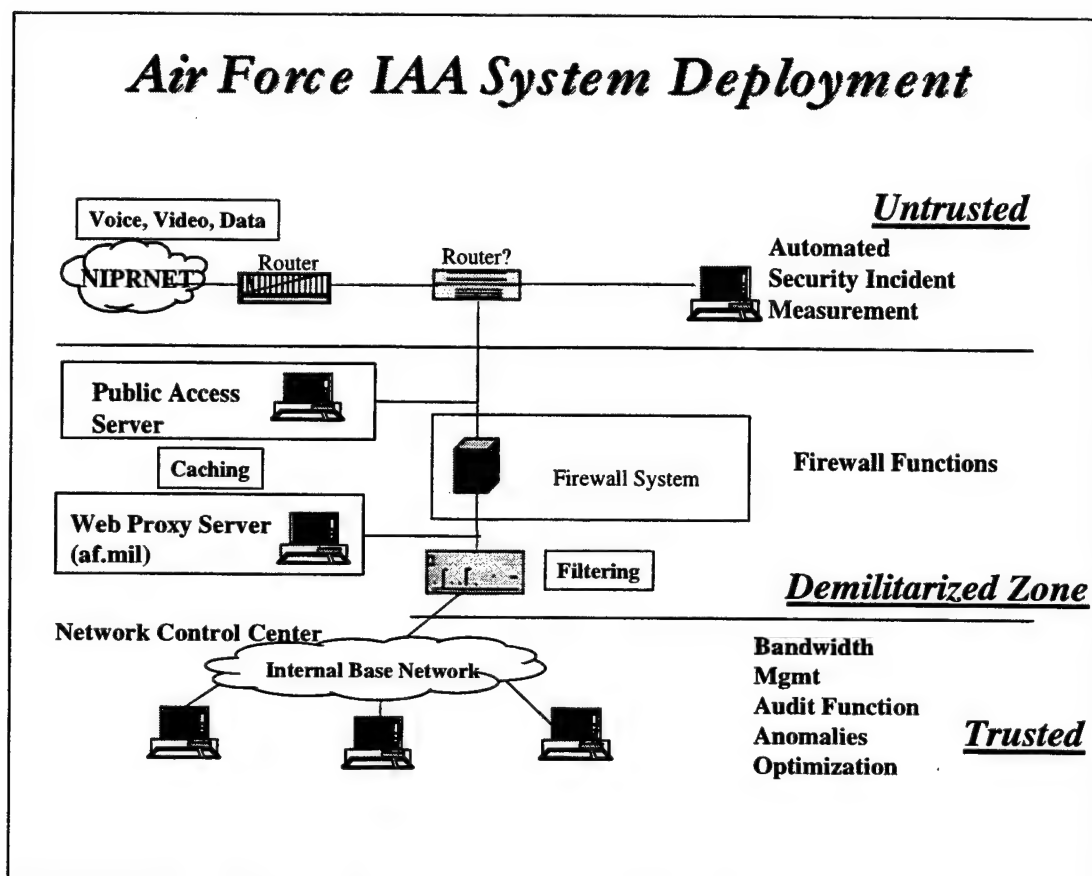


Figure 18. Air Force IAA System Deployment

The Air Force has taken an alternative approach to implementing DiD as compared to the Army. As shown in Figure 18, the Air Force is deploying different protocol translation architecture as well as different locations for performing its enclave-level intrusion detection. Furthermore, the Air Force has combined both firewall and router filtering to provide access control to their enclave infrastructure.

The Air Force implementation is, however, similar to the Army's in that they both invite the general public into their enclave DMZ's for general information services. Thus, the general public is required to transit the NIPRNET for these services; everyone on the WWW is an "insider" on the NIPRNET, with access control being levied only at the installation boundary. Malicious behavior detection for both the Army and the Air Force is conducted at the common access point to the DMZ information services and at the Army/Air Force installation (managed) services. In both cases, the general public can reach this access point as well as the access points associated with the actual installation boundaries.

The Navy's IAA is to be determined (TBD). The Navy has chosen to outsource its GIG/Intranet, including IA services. The Navy does have concepts for how to protect its enclaves, but it has decided to procure IA as an incentivized service in the acquisition. The panel was not able, therefore, to comment on the IA system architecture that the Navy will have. What is evident, however, is that each service is pursuing its own solution to the problem of providing IA for its specific GIG/Intranet component of the DoD NIPRNET VPN. Each service's solution is different and attendant interoperability issues will arise given that all components must be integrated into the NIPRNET. Intrusion Detection System (IDS) information must be readily shared as must information to dynamically set filtering in firewalls and routers given indicators and warnings of information operations against the DoD GIG. Such coordination is especially difficult in the context of diverse defense-in-depth implementation strategies.

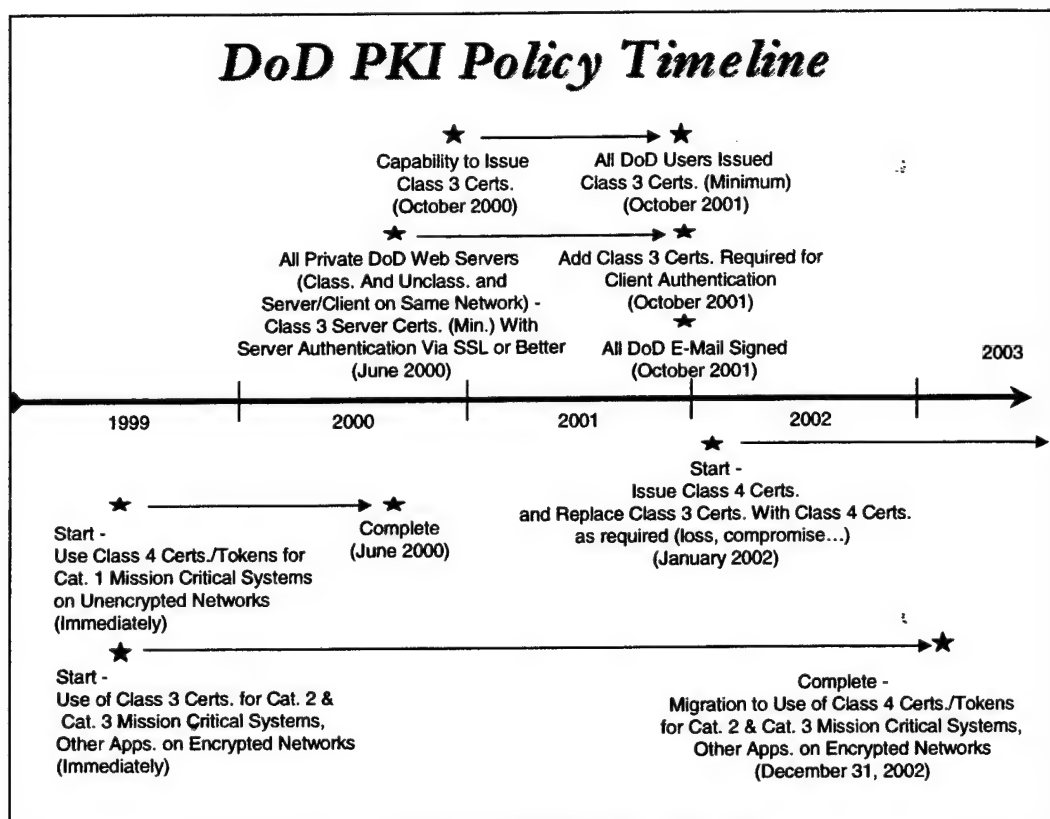


Figure 19. DoD PKI Policy Timeline

An important element of the DoD IAA system architecture is the deployment and use of commercial-based public key infrastructure (PKI). Figure 19 depicts the current DoD PKI policy timeline. This policy applies to all DoD components and provides timelines for the issuance of class 3 and class 4 PKI certificates.

Class 3 certificates are designed to protect administrative, mission support, and some mission-critical information when being transferred within a single security classification level. Class 3 certificates can be issued with a private key contained in a software token. Class 4 certificates protect sensitive but unclassified mission-critical information passing over

unencrypted networks, and the corresponding private keys are intended to be contained in hardware tokens.

The policy establishes timelines for issuing class 3 and 4 certificates to users. It also establishes the timeline for using certificates for web server access control and for email. The timeline shown above has dates that are not aligned with the Common Access Card (CAC) program. The CAC program will provide, via the Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System (DEERS/RAPIDS), the ability to issue smart cards to DoD personnel that can contain at least class 3 certificates. It is anticipated that class 4 certificates may be able to be issued via the CAC, though this policy was not yet in place at the time of this study. Because the current PKI timeline is not aligned with the CAC timeline, a new PKI policy has been drafted. Though not yet finalized, this policy is expected to move the June 2000 dates to December 2000.

3.3 OPERATIONAL ARCHITECTURE

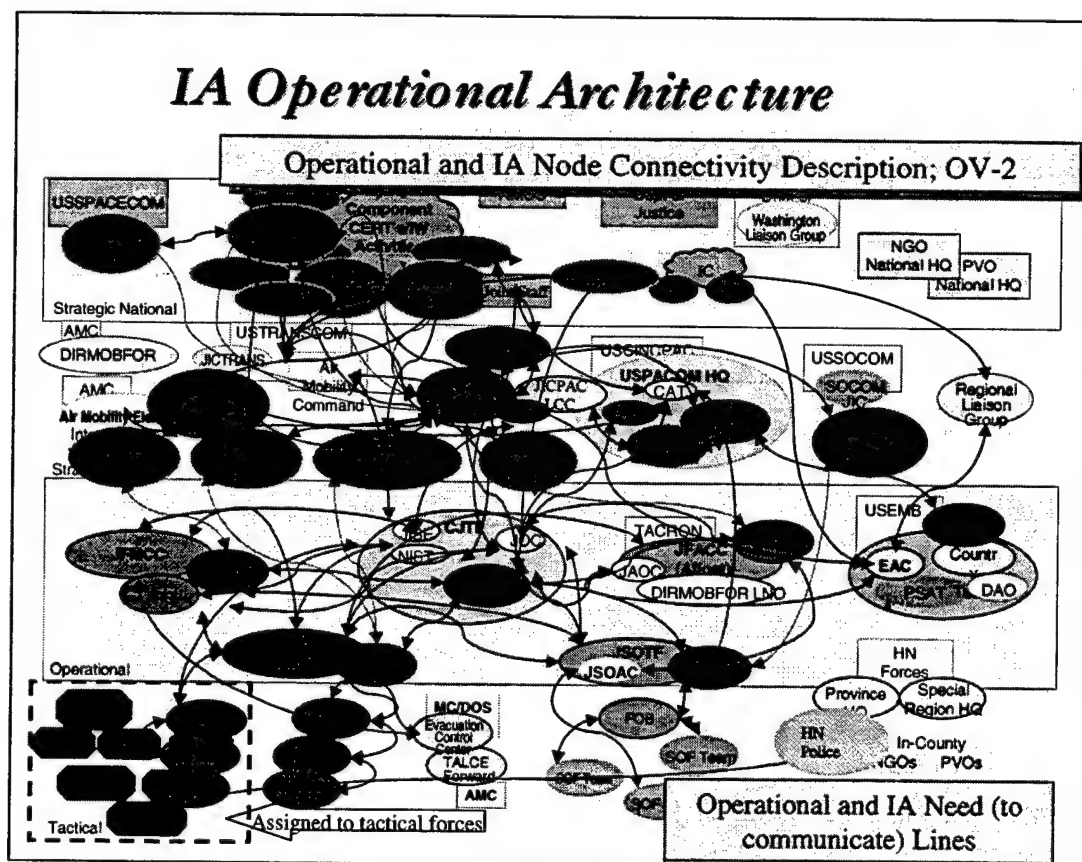


Figure 20. IA Operational Architecture

In addition to the progress made in establishing an IAA system architecture, DoD has begun the process of establishing an IAA operational architecture. Figure 20 depicts one product that has resulted from this effort to date. In this figure, operational facilities (OPFACs) that would be involved in IO processes are identified. The IAA OA has also identified the IA-related

information exchange requirements (IERs) between these OPFACS that is necessary to coordinate and conduct IA activities. The figure represents a limited non-combatant evacuation operation (NEO), height-of-operation, scenario in the Pacific.

As part of the operational architecture effort, information exchange metrics, activity models, and logical data models are being developed. The panel noted that this IA operational architecture effort is important and will make a critical contribution to understanding IO mission processes, responsibilities, and required information flow for specific concept of operations. Furthermore, this operational architecture will be important in helping to define how IO can/should be process-reengineered to allow for more efficient and timely response to IO missions and threats in the future.

Although establishing an IA operational architecture is a difficult and time-consuming task, the panel feels this effort will provide important insights into the mission, organization and tactics, techniques and procedures (TTPs) required to effectively execute IO. For example, the panel noted that the number of OPFACs associated with the limited scenario represented in Figure 20 implies a substantial IO coordination and information exchange overhead in support of the mission. From such "as-is" operational architecture efforts, "to-be" architectures can be investigated that would simplify the prosecution of IO missions to achieve information superiority as envisioned in JV2020. It is noted, though, that a single IA operational architecture is not sufficient. A representative set of IAA operational architectures for various types of missions and areas of responsibility should be developed in order to more fully understand the entities, processes, and supporting IERs for IA.

3.4 TECHNICAL ARCHITECTURE

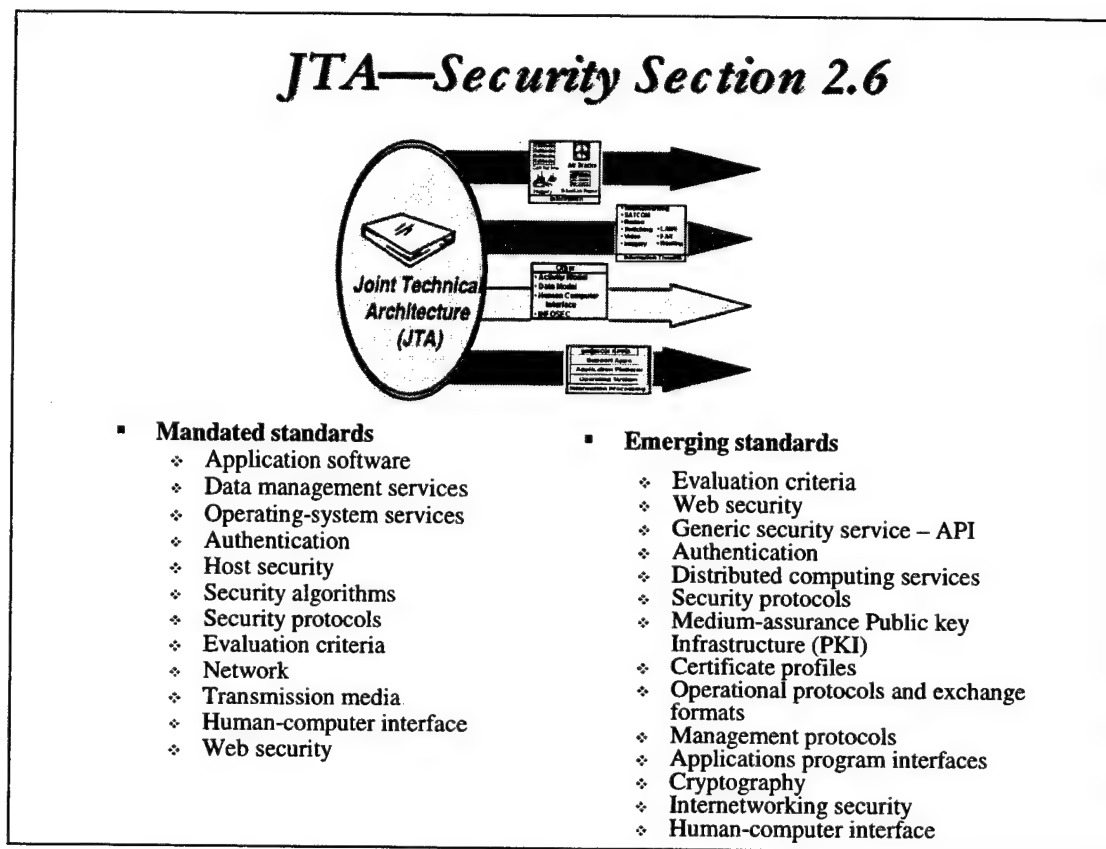


Figure 21. JTA—Security Section 2.6

The remaining component of the IA architectural framework is an associated technical architecture. This latter component is the third element of the DoD C4ISR architectural framework methodology. The set of IA architectural components, IA operational architecture (IA-OA), the IA system architecture (IA-SA), and the IA technical architecture (IA-TA), will provide the perspective to support securing and protecting the Global Information Grid.

The panel received two briefings on IA-TAs. The first was a briefing on Section 2.6 (Security) of the DoD Joint Technical Architecture (JTA). The JTA identifies the services, interfaces, standards, and their interlocations and provides the technical guidelines for implementation of information systems and services. The standards selected for the JTA are selected primarily from the private sector IT industry although some military specific (MILSPEC) standards are included where no commercial counterpart exists. Figure 21 provides a summary of the JTA security chapter.

The panel noted that the standards called out in the JTA for mandated standards are consistent with those noted in the ISO security reference model presented previously. The concept, processes, and content of the JTA, and specifically Section 2.6, are strongly endorsed by the IAA Panel.

Standards & Protocols for Providing Security to System Applications from IATF (Inconsistent with JTA)

- | | |
|--|---|
| <ul style="list-style-type: none"> ▪ Application Layer <ul style="list-style-type: none"> ✦ Secure HyperText Transfer Protocol (S-HTTP) ✦ Object Management Group's Common Object Request Broker Architecture (CORBA) ✦ W3C XML Transfer Protocol ✦ Secure FTP (S-FTP) ✦ Secure Electronic Transactions (SET) ✦ Message Security Protocol (MSP) ✦ Secure/Multipurpose Internet Mail Extensions (S/MIME) ▪ Transport & Network Layer <ul style="list-style-type: none"> ✦ Transport Layer Security (TLS) ✦ Secure Socket Layer (SSL ver 3.0) ✦ Secure Shell (SSH) ✦ Internet Protocol Layer Security (IPSec) ▪ Data Link Layer <ul style="list-style-type: none"> ✦ Point-to-Point Protocol (PPP) ✦ Serial Line Internet Protocol (SLIP) | <ul style="list-style-type: none"> ▪ Security Management Infrastructure <ul style="list-style-type: none"> ✦ Internet Engineering Task Force (IETF) Public Key Infrastructure ✦ IETF Simple Public Key Infrastructure (SPKI) ✦ IETF Domain Name System Security (DNSSEC) ▪ Data Labeling <ul style="list-style-type: none"> ✦ National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 188 Standard Security Label ✦ Institute of Electrical and Electronics Engineers (IEEE) 802.10 g Secure Data Exchange (SDE) Security Label ✦ IETF Internet Security Label ✦ International Organization of Standardization (ISO) SC-32 Security Label ✦ Military Standard (MIL STD) 2045-48501 (Common Security Label) ✦ SDN.801 Reference Security Label ✦ ISO MHS.411 Security Label |
|--|---|

Source: IATF, Section 7.1.1.5

Figure 22. Information Assurance Technical Framework

The second technical architecture briefing to the panel concerned the Information Assurance Technical Framework (IATF), an excerpt of which is provided in Figure 22. The panel found this document to be a tutorial and collection of useful generic information on IA. The panel noted, however, that the section of the IATF associated with standards and protocols for providing security to system applications is incorrect and inconsistent with the JTA. The IATF, unlike the JTA, is not a standards setting or selection document. Rather, the IATF Forum has been organized to encourage participation by vendors of (largely COTS) IA products and services. The major focus of the IATF is the development of protection profiles (under common criteria) that will be used to evaluate products, i.e., under the national Information Assurance Partnership (NIAP) program operated by NIST and National Security Agency (NSA). There is no unified architectural underpinning for the IATF. This is to be expected, i.e., security evaluation criteria such as the Common Criteria (CC) (and product profiles based on the CC) tend to be architecture independent. As a result, the collection of standards cited by the IATF, as briefed to the panel, lacks architectural continuity and it is not an appropriate alternative to the work of the JTA.

Many of the security standards that are collected in the IATF are experimental or did not gain acceptance in the Internet. For example, secure hypertext transfer protocol (S-HTTP) is not implemented in any commercial browsers or servers; it lost the protocol battle to SSL/TLS. SPKI is not a standard, but rather is the experimental output of a failed IETF working group, not

supported in commercial products. The Public Key Infrastructure Working Group (PKIX WG) of the IETF produces standards based on X.509, which are implemented in a wide variety of products. Moreover, the other IETF security protocol working groups make use of the PKIX standards, not SPKI. The IATF referenced a wide range of security labeling standards that are a mix of redundant and/or superceded documents.

The IATF thus suffers from the same problems associated with the TAFIM; it is a collection of history and general information – not a document that can be used to implement interoperable, secured information systems for DoD.

The panel notes, with concern, that DoD policy requires that the JTA be used as the “building code” for the DoD information infrastructure. On the other hand, the recent document from the Deputy Secretary of Defense, subject “Department of Defense Chief Information Officer Guidance and Policy Memorandum no. 68510,” Department of Defense Global Information Grid Information Assurance (ASD/C3I) suggests that the IATF and published Common Criteria Protection Profiles be consulted “for guidance... and IA solutions that should be considered to counter attacks.”

The panel’s concern is the apparent confusion these two policy statements could cause within the IA community. The IATF standards are incorrect and inconsistent with the JTA and private sector practice. The panel believes the JTA is the better reference on IA standards and protocols, and it should be referenced as such in all GIG IA policy documents.

3.5 METRICS

Joint Staff J6, IA Metrics

- Performance-based
- Integrated into operational readiness reporting
- CINC's report as part of JMRR process
- Example

INFORMATION ASSURANCE METRICS (List 1)				
1.0	PLANS AND OPERATIONS			
Joint Readiness: C-Level	PLANS AND OPERATIONS ASSESSMENT			
C-1 minor deficiencies with negligible impact on capability to perform required missions.			
C-2 some deficiencies with limited impact on capability to perform required missions.			
C-3 significant deficiencies ... prevent it from performing some portions of required missions.			
C-4 major deficiencies that preclude satisfactory mission accomplishment.			
1.1	Plans — Planning involves both those specialized IA plans and IA portions of operations plans. IA Planning should identify necessary resources in detail.			
1.1.1	IA portion of concept of operations and operations plans; standard operating procedures (SOP), continuity of operations plan developed and effectively implemented.	C1	C2	C3 C4
1.2	Operations — ongoing execution of daily IA support procedures....			
1.21	Garrison Operations —IA strategy should support military operations			
1.21.1	IA integrated sufficiently in current/ongoing operations	C1	C2	C3 C4
1.2.2	Deployed JTF operations			

Figure 23. J6 IA Metrics

As noted in the GIG reference material (see Figure 6), metrics play an important role in architecting and deploying this infrastructure. The panel, therefore, chose to address this topic as a stand-alone topic outside of the DoD C4ISR architectural framework. Only two specific initiatives addressing IA metrics with DoD were presented to the panel. They are described next.

Figure 23 provides an overview of IA operational readiness metrics developed by the Joint Staff. These metrics are used by the CINC's to assess and report on IA readiness as part of their overall readiness assessment. The panel noted that these metrics are a good starting point to raise the awareness and importance of IA as a critical warfighting requirement. Although these metrics are difficult to measure, are not yet comprehensive in nature, and do not address the CINC's warfighting capabilities as supported or hindered by the IA capabilities, they do raise IA awareness within a CINC's organization, and they do begin to raise the importance of IA to the warfighter. The panel recognizes that this set of metrics will evolve and improve over time.

Assessment Framework Notional Metrics Criteria

- Defense-wide Information Assurance Program Initiative
- Goal: Operationalize IA readiness
- Objectives:
 - ❖ Define IA readiness in operational context
 - ❖ Establish metrics for measuring IA readiness
 - ❖ Establish standard criteria for applying IA readiness metrics
 - ❖ Establish IA readiness assessment process
 - ❖ Integrate IA readiness assessment into existing DoD processes
- Examples:

Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
People	Adequacy of IA Personnel Manning Levels	Adequacy of IA Personnel Manning Levels	1. All IA billets must be designated per DoD policy xxxx 2. All IA billets must be accounted for	The following billets are identified as IA billets	C1	90% manned, replacements identified for outbound personnel
					C2	90% manned, replacements not identified for outbound personnel
					C3	75% to 89% manned
					C4	Less than 75% manned

Figure 24. Assessment Framework

The second initiative on establishing IA metrics is being conducted under the auspices of the Defense-wide Information Awareness Program (DIAP). A team has been established and is tasked to develop an IA readiness assessment framework and associated metrics. The team has begun the process of defining quantifiable IA metrics and associated ratings, as indicated by the example in Figure 24. The panel noted that the metrics presented by the speaker overlapped to some degree with those presented by the J6 briefer. The panel understood that the J6 metrics are intended to be integrated with the DIAP metrics in a process that will provide a DoD-wide IA readiness assessment.

Based on the two briefings, however, the panel felt that greater coordination is necessary between the two efforts. The message conveyed by the speakers tended to leave the impression that these efforts were not tightly coordinated, could lead to duplication of effort, and, of greatest concern, could lead to confusion within the user organizations that are being assessed.

The panel felt that a single DoD IA effort should exist that addresses the spectrum of IA metrics that are necessary. This spectrum is much greater than the sets of metrics presented by the J6 and DIAP. For example, IA technology and system-architecture related IA metrics should also be developed and used to assess progress and residual vulnerabilities in the GIG as it is deployed and improved over time. The panel could identify no specific, focused initiative on developing such technical metrics. The panel's suggestions regarding metrics are provided in the next section of this report.

3.6 WIRELESS

The panel noted that wireless-infrastructure IA issues were not raised in any of the briefings it received. Although wireless data communications over military owned/operated systems is well understood and IA is typically provided through transmission security (TRANSEC) at the physical layers and communication security (COMSEC) at the application layer, the private sector wireless infrastructure that today is embedded in the GIG was not addressed as an area of concern within DoD. The panel notes that private sector wireless media can be used as a means to gain access and control of the "wired" part of the commercial infrastructure (at network management layers). This wireless segment of the infrastructure must be carefully protected. As a result, this issue is addressed in greater depth in the next section of this report.

DSB IAA Matrix of Recommendations		
Source: Report of the Defense Science Board Task Force on Information Warfare - Defense (IW-D) (November 1996)		
Assess infrastructure dependencies and vulnerabilities.		X
Define threat conditions and responses.		X
Assess IW-D readiness.		
"Raise the bar" with high-payoff, low-cost items.		X
Establish and maintain a minimum essential information infrastructure.		X

Figure 25. DSB IAA Matrix of Recommendations

3.7 SUMMARY OF FINDINGS

As part of our findings, the panel notes that the 1996 DSB Summer Study made four overarching recommendations related to IAA. These recommendations are listed in Figure 25. From the preceding discussion, the panel makes the following observations.

Recommendation 1: Assess infrastructure dependencies and vulnerabilities. The DoD today is relying primarily on the private sector to assess NIPRNET infrastructure dependencies and vulnerabilities. As vulnerabilities are identified, the DoD implements the associated fixes within the NIPRNET (software patches, virus filtering, IDS templates) using DiD as the basis for its system architecture. However, the panel notes that there is currently no methodology for "engineering" DiD. There are processes for implementing DiD updates, but there is no engineering discipline that allows for the design of a DiD solution with confidence in the security

it offers in the face of various threats. The premise underlying DiD is that an acceptable level of protection can be achieved through layering of defenses, even though each defensive technology is known to be imperfect, i.e., each one is known to have residual vulnerabilities or functional shortcomings. Also, central to the DiD premise is the assumption that each layer of defense exhibits functional deficiencies or vulnerabilities that are independent (ideally orthogonal), and thus the ability to penetrate one defensive layer does not imply the ability to penetrate other layers (by the same means). However, to the extent that many of these defenses are built upon COTS operating systems (OS) that are known to be vulnerable, but for which not all residual vulnerabilities are known, this premise is questionable. Moreover, not all the flaws in each defense mechanism are likely to be known because they are COTS products with low to medium assurance. Thus it is not possible to estimate the extent to which such layered defenses increase the work factor for an attacker, above and beyond the OS problem cited above. (Nonetheless, there is reason to believe that the work factor is increased, at least for low-grade threats.) None of these observations implies that DoD should not pursue DiD. Rather, they suggest that additional effort is needed to develop a suitable methodology that will support DiD engineering and deployment. They also suggest that prospective users of a DiD strategy should be apprised of the uncertainty associated with both the strategy and its implementation.

Recommendation 2: Define threat conditions and responses. The DoD information condition (INFOCON) policy and procedures are well established, promulgated and understood. The panel does not believe, however, that DoD has experience in understanding (how consistent and timely the responses will be executed throughout DoD) upon INFOCON status changes. Furthermore, the panel believes that experience is lacking in assessing how effective the INFOCON procedures will be in thwarting an attack. Gaining this experience, through continuous exercises and the assessment of INFOCON responses to varying red-team attacks, is an important process to establish.

Recommendation 3: "Raise the Bar" with high-payoff, low-cost IA Initiatives. The panel notes that a great deal of progress has occurred here as well. DoD has established an IAA framework, it has selected a systems architecture, and it is deploying DiD solutions; it has increased user/community awareness of the IA problem. The panel does note, however, that work remains to be done. Simple but strict IA configuration management practices at all DoD information sites is still a critical issue; closing all NIPRNET connections to the public Internet (other than through the 8-11 DoD gateways) remains an unresolved issue; and the insider threat on the SIPRNET and JWICS remains an open issue although suitable IA technologies and processes to mitigate this risk are available.

Recommendation 4: Establish and maintain a minimum essential infrastructure. The panel did not receive any indication that this recommendation was being pursued by DoD. In fact, DoD has focused on deploying a GIG with integrated IA services. The panel does support the goal of deploying and securing the GIG, but notes the following: the GIG is being deployed based on a security strategy referred to as "risk management," not one aimed at achieving an impenetratable minimum essential in infrastructure. It has been suggested that, in the past, security experts focused on achieving "perfect" security, which can be viewed as a "risk avoidance" strategy. In fact security experts have long acknowledged that perfect security is unattainable. Risk management argues for explicitly making a decision to accept a certain level of risk as a condition of deploying a system. This is a fine principle, but it is based in part on the

premise that one can evaluate (and quantify) the residual risks associated with a system composed of components that are known to be imperfect. This is a questionable assumption. First, although one might be aware of some set of residual vulnerabilities in the system components, it also is likely that these components contain other, unknown vulnerabilities of undetermined severity. Second, there is no algebra that allows the computing of the risk associated with deploying a system composed of components with known vulnerabilities, much less a system in which the components have unknown vulnerabilities. Thus it seems certain that risks of unknown magnitude are being accepted when the phrase "risk management" is part of the security design and accreditation process. This issue can, at this time, only be addressed through empirical means whereby a representative segment of the deployed GIG is subjected to a comprehensive and continuous IA vulnerability assessment process. A "testbed" concept will be proposed in the next section as a means to address this need.

GIG IA: Summary of Findings

- GIG today = NIPRNET + SIPRNET + JWICS + Service Tactical C3I systems
 - ❖ All transit commercial communication media (including wireless)
 - ❖ All leveraging commercial IT
 - ❖ All cryptographically segmented into virtual networks
 - ❖ Insider threat not addressed (special concern in JWICS/SIPRNET)
- Multiple efforts causing some confusion and misdirection
- Rigorous, consistent DiD engineering not occurring
- Immature IA metrics address only force readiness
- Denial of service and attack attribution not well addressed
- Mobile code still an issue but a critical future technology

Absent an office of primary responsibility, the GIG will not achieve joint weapons system status

Figure 26. GIG IA Summary of Findings

In closing this section of our report on panel findings, Figure 26 provides a summary of our observations. The Global Information Grid does comprise multiple virtual worldwide data networks, the NIPRNET, SIPRNET, JWICS and service tactical C3I systems. These networks use shared commercial communications media and commercial information technologies. In addition, all are cryptographically segmented into virtual networks. However, the panel noted that there is virtually no protection against the insider threat, especially for the classified networks. All services are adopting a Defense-in-Depth (DiD) strategy, with different

implementations. For example, the Air Force is employing a different strategy from the Army: a different protocol translation architecture; a different location for performing enclave level intrusion; and different measures for enclave access control. The panel notes that while there is a general framework for implementing DiD, there is no engineering discipline that allows for design of a DiD solution that provides confidence in security against a variety of attacks.

The current emphasis on information assurance metrics is focused on readiness and is not addressing the metrics needed to assess and measure mission, system or technical level performance. In addition, denial-of-service measures and attack attribution metrics are not well addressed.

Finally, the panel believes that today's DoD organizational structure is inadequate to deliver a GIG. Although both the DoD Chief Information Officer (CIO) Executive Panel and the Military Communications and Electronics Board (MCEB) are working on defining and providing guidance for the GIG, the panel feels that a new organizational structure, with a centralized primary point of responsibility, will be required to develop a GIG worthy of weapons system status.

Specifically, the current charter of the DoD CIO Executive Board is contained in the DepSecDef Memo Subj: DoD Chief Information Officer Executive Board, 31 March 2000. This charter states that the Council is the principal forum to advise the DoD CIO on the full range of matters pertaining to the Clinger-Cohen Act (CCA) of 1996 and the Global Information Grid. Additionally, the board also coordinates implementation of activities under the CCA, and exchanges pertinent information and discusses issues regarding the GIG, including DoD information management (IM) and information technology (IT). The primary mission of the board is to "advance the DoD's goals in the areas of IM, information interoperability and information security between and among Defense Components." The Board also coordinates with the IC CIO Executive Council on matters of mutual interest pertaining to the GIG. Its management oversight includes recommending, reviewing, and advising the DoD CIO on overall DoD IM policy, processes, procedures and standards, as well as overseeing all aspects of the GIG to support the DoD's and IC's mission and business applications. This includes the collaborative development of IT architectures and related compliance reviews; management of the information infrastructure resources as a portfolio of investments; collaborative development of planning guidance for the operation and use of the GIG; and identification of opportunities for cross-functional and/or cross-component cooperation in IM and in using IT. The board's architecture management responsibilities include ensuring the collaborative development of architectures as specified in the CCA, and ensuring that processes are in place to enforce their standardized use, management and control, as well as aligning IT portfolios with the GIG. Although the board has budgetary review authority for IT investments, and can make recommendations, it has no direct budgetary authority. It also has no authority, either review or management oversight, over the warrior components of the GIG. The membership of the DoD CIO Executive Board includes:

- Chair: DoD CIO (ASD (C3I))
- Members: CIOs of the Military Departments
 - CIO, Joint Staff

- USD (AT&L)
- USD (P) (Policy)
- USD (C) (Comptroller)
- USD (P&R) (Personnel and Readiness)
- ASD (C3I) (usually the Deputy CIO)
- Director PA&E (Program Analysis and Evaluation)
- J6, Joint Staff
- OPNAV N6
- Director, Communications and Information, USAF, AF/SC
 - IC CIO
 - CIO, JFCOM (Joint Forces Command)
- Security Advisor: Director, National Security Agency (DIRNSA)
- Technical Advisor: Director, DISA
- Legal Advisor: DoD General Counsel

The charter of the MCEB is contained within DoD Directive 5100.35 dated 10 Mar 1998. The MCEB considers those military communications-electronic matters, including those associated with national security systems (NSS) referred to it by the SecDef, CJCS, the DoD CIO, secretaries of the military departments, and heads of DoD components. The mission of the MCEB is to obtain coordination among the DoD components, between the Department of Defense and other governmental departments and agencies, and between the DoD and representatives of foreign nations on matters under the MCEB jurisdiction. The MCEB provides guidance and direction to the DoD components and advice and assistance as requested. The membership, as listed below, is primarily composed of those in charge of the communications activities in the listed components, which have little, if any, authority over IT issues in other portions of their component. The MCEB has no budgetary review or execution authority over any component, nor is there any mechanism within the MCEB structure for enforcement of non-compliance with decisions. The relationship between the MCEB and CIO Executive Board is still being discussed, but in effect, the MCEB is a subordinate activity under the direction of the CIO Executive Board and its recommendations are referred to that Board for final decision. Membership of the MCEB includes:

- Chair: Joint Staff, J6
- Members: Vice, J6
 - DISC4, U.S. Army
 - OPNAV, N6
 - HQ USAF, SC
 - HQMC, C4
 - USCG, Assistant Commandant for Systems
 - Director, DISA

- Director, NSA
- Director, DIA

Thus, neither the DoD CIO Executive Board nor the MCEB has the membership or authority over budgets and execution activities that the panel believes are necessary to ensure the GIG is built and managed as intended by the IAA Panel. Without that level of authority over all elements of the GIG, the architecture is subject to interpretation by each component based on its needs, rather than the needs of the entire DoD enterprise. There is also little incentive to address crosscutting issues in a coherent fashion when the funding for these programs is provided via Title 10 channels without some mechanism to encourage cooperation. Because of the Title 10 and DoD versus intelligence community issues, the only level of management senior enough to cross this bridge is at the DepSecDef level. Additionally, neither of these two boards has a direct oversight responsibility over any specific office or organization that carries out its direction.

CHAPTER 4. "WHAT MIGHT BE DONE" PANEL SUGGESTIONS

4.1 THE GIG IS A WEAPON SYSTEM

The GIG is a Weapon System

- It leads to information/decision superiority, therefore it will be attacked by our adversaries
- Built unlike a traditional weapons system
 - ❖ Critical elements not owned by the DoD
 - ❖ A platform shared by all DoD users
 - ❖ Built primarily from COTS components
 - ❖ Components evolve very rapidly
- Attacked more readily
 - ❖ Low "cost of entry" for attackers
 - ❖ Easy to deny service globally
 - ❖ Attacks escalate rapidly (compressed Observe, Orient, Decide, Act [OODA] loop)
 - ❖ Attack attribution is difficult
 - ❖ Forensics processes & technology are immature

Figure 27. The GIG is a Weapon System

Information superiority is the pacing item in realizing the goals of JV2020, and the Global Information Grid is the underlying information superiority infrastructure. The panel argues, in Figure 27, that because of its importance, the GIG should be viewed as a weapons system, one that will present a lucrative target for our adversaries. However, unlike traditional weapons systems, the critical elements of the GIG are not owned or controlled by the DoD. Furthermore, the GIG is shared by all DoD users and is built primarily from COTS components, which are rapidly evolving.

A significant weakness of the GIG is that it can be more readily attacked than traditional systems, which are far less ubiquitous and have limited interfaces and stricter controls. This is due to several factors, but first and foremost is the low capital cost of entry for attackers. A few people with personal computers and Internet access have demonstrated the capability to deny

service and penetrate DoD systems. Attacks have a non-linear characteristic in that they can escalate rapidly, as evidenced by the recent distributed denial-of-service attacks. Unfortunately, attacker attribution is difficult if not impossible today. The attacker enters third party machines and uses those facilities to launch attacks. Current processes and forensics for identifying and tracing attackers are primitive and do not provide adequate support for attribution.

Assumptions for IAA Suggestions

- DoD establishes the Internet Protocol (IP) as the convergence layer for information services on the GIG
 - ❖ Private sector parallel
 - ❖ Recommended in DSB Tactical Battlefield Study*
- DISA migrates Defense Information Infrastructure (DII) from native ATM backbone to IP services
 - ❖ Requires development/deployment of high-speed (Gigabit) IP network encryptors

* Reference: DSB Task Force Report on Tactical Battlefield Communications, February 2000

Figure 28. Assumptions for IAA Suggestions

Figure 28 provides the assumptions that are the foundation of the panel's IAA suggestions. These assumptions are based on the following. In the private sector, a trend is underway to develop a single infrastructure providing integrated voice, video and data services. This trend to a common, shared infrastructure for all multimedia services is termed "convergence." The convergence is facilitated by and expected to occur through a common, ubiquitous protocol – IP. This protocol is an open standard supported worldwide by the data telecommunications industry; it is rapidly becoming the convergence layer for all information services on the Internet.

The common IP layer separates the task of telecommunications (transport) from the tasks of service types, information types, and application development. Network engineers concentrate on moving IP packets from one place to another, independent of their content. Application and service developers concentrate on applications and count on the IP layer to provide requested telecommunications services.

The present version of the IP, designated Internet Protocol Version 4 (IPv4), does not yet support QoS-based dynamic resource allocation, a capability needed to support real-time, stream-oriented information flow (i.e., real-time voice and video). In the near term, this limitation is being addressed through higher-layer protocols such as the Real-Time Protocol (RTP), and the Resource Reservation Protocol (RSVP) and via tag switching. In addition, extensions to IPv4, to include a minimum level of QoS, are being investigated by the Internet Engineering Task Force (IETF). The IETF is also working on the next generation of IP, called IPv6, which will include QoS (called differentiated services) and a much larger IP address space, permitting the integration into the Internet of embedded processors (sensors) and many more addressed devices as users.

Today IP is used over many dissimilar networks including: ATM, Ethernet, wireless 802.11, Cellular Digital Packet Data (CDPD) and the like. IP was designed to be the mechanism for transparently moving bits across such networks. Thus, IP is the mechanism that permits the integration of these many types of networks into a network-of-networks – that is, the Internet.

The panel noted that a prior DSB study made a strong recommendation that DoD establish IP as its convergence layer for the GIG.⁶ In our discussions with DISA, the briefer observed that he was strongly in favor of migrating the Defense Information Infrastructure (DII) to an IP service infrastructure, resulting in IP being the standard interface to the DISA-supplied point of presence (POP) at all DoD sites supported on the DII. This migration would place DII in the mainstream of the private-sector migration toward a converged infrastructure. Thus, DoD, through DISA services, could fully take advantage of private sector IT.

It was noted that to support this migration, DISA would need high-speed, Type 1, IP network encryption technology. Today DISA uses ATM encryptors developed by DoD, given that DISA provides ATM service to POPs. The panel noted that DoD is supporting the development of equivalent IP devices.

Thus, the panel assumes, in what follows, that DoD will migrate to IP as its convergence layer for the GIG. By doing so the DoD benefits significantly not only in leveraging commercial IT transport technology and services, but also from the perspective of leveraging emerging private-sector IA and IAA technologies, protocols and services.

⁶ Reference: Defense Science Board Task Force Report on Tactical Battlefield Communications, February 2000

4.2 ARCHITECTURE SUGGESTIONS

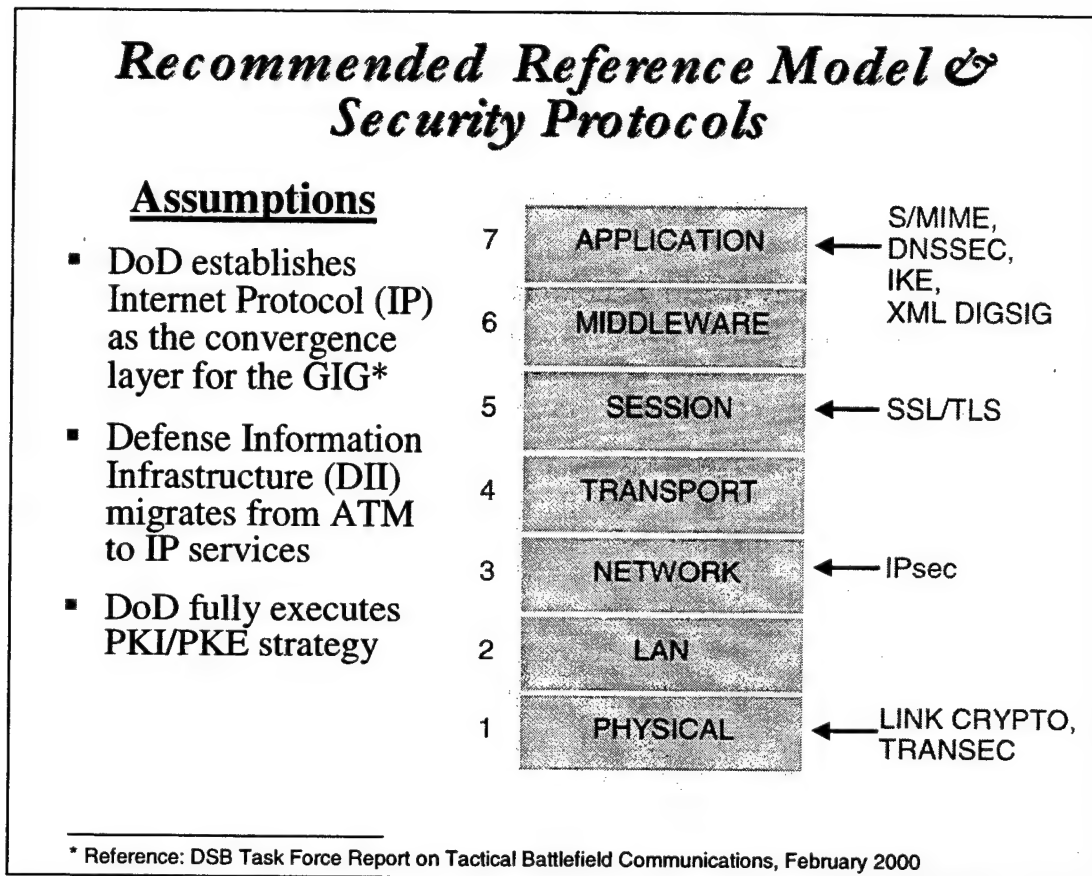


Figure 29. Recommended Reference Model and Security Protocols

The panel's suggested IA reference model is shown in Figure 29. This protocol stack assumes the use of internet protocols in a wide range of environments, including both tactical and strategic. It parallels the ISO reference model (ISO 7498), with the substitution of a "middleware" layer in lieu of the presentation layer, and is consistent with the TCP/IP protocol suite. (This substitution seems appropriate because modern systems do not make use of separate presentation layer functions; these functions are assumed by applications.)

Physical layer protection is afforded via link cryptographic systems (i.e., KG 84, KG 189, etc.) on a hop-by-hop basis, where warranted by threat concerns. No data link security; i.e., LAN security protocols such as IEEE 802.10, is recommended. This technology has not been adopted by product vendors and is generally not warranted in switched LANs, when higher layer security protocols are employed. IPsec is recommended for end-to-end, enclave-to-enclave, or end-to-enclave protection. No transport (i.e., TCP) layer security protocol is recommended because there are no widely used standards yet available, and because the services provided at the IP and session layers obviate the need for transport layer security.

Although the Internet protocol stack does not include a session layer per se, the introduction of SSL, SSH, and analogous security protocols has created one. SSL is widely deployed and DoD policy calls for its use for secure web access. We recommend its use with client (not just server) certificates, for high quality user authentication and access control, with transition to TLS (the IETF standard) as it becomes more widely available.

The panel has inserted a "middleware" layer to accommodate systems such as Common Object Request Broker Architecture (CORBA), distributed computing environment (DCE), or Enterprise Java Beans (EJB). However, such systems are not universally required and there is no clear appropriate choice among these competing middleware technologies at this time. Finally, several critical protocols exist at the application layer, and more may emerge. For secure e-mail, S/MIME (v3 with enhanced security services) is the preferred protocol, and it is widely available in COTS products. Secure DNS is an essential infrastructure security component requiring DISA as well as base-level support. Internet Key Exchange (IKE) is the key management protocol used by IPsec. As the extensible markup language (XML) becomes more common, the digital signature standards developed for it will become critical elements of more sophisticated web security designs, supplementing, but not supplanting, SSL/TLS.

GIG IA/SA Strategies

- **Discipline implementation**
 - ❖ Use consistent architectural framework & metrics
 - ❖ Ensure interoperability via commercial standards
- **Segment the communities**
 - ❖ DoD vs. general public, by classification, by enclaves (COI), by user authorization within enclave
 - ❖ Invest in PKI/PKE & high speed, inline IP encryption
- **Counter denial of service**
 - ❖ Use segmentation, redundancy, diversity, restricted set of Internet access points, & non-switched commercial infrastructure
 - ❖ Improve net infrastructure security (e.g., S-BGP)
- **Enhance indicators, warnings, and attribution**
 - ❖ Correlate multi-layered IDS outputs, use as inputs to intelligence-enabled tracing systems
modus operandi detection
 - ❖ Use PKI to increase S/N ratio

Figure 30. GIG IA Strategies

Figures 30 and 31 outline the GIG IA system architecture strategies recommended by the panel, representing the underlying themes that are embodied in the later recommendations. The first strategy is to use a consistent architectural framework and metrics across the entire DoD

GIG. This strategy lies in contrast to the current divergence of approaches between the services. It is important to foster interoperability via commercial standards, so that commercial and government off-the-shelf technology can be employed throughout the system. The defense-in-depth approach leads to the strategy of segmentation. Segmentation is recommended between the DoD and the general public Internet, between levels of classification, by enclaves (COI), and by individual user within an enclave. In order to support segmentation, investment will be needed in high-speed in-line IP encryption devices, and in large scale PKI and PKE.

Segmentation, redundancy, diversity, a restricted set of Internet access points, non-switched commercial infrastructure, and improved overall net infrastructure security, such as S-BGP (Secure Boundary Gateway Protocol), used in concert can partially mitigate the denial-of-service threat.

Another important element of the strategy is to enhance indicators and warnings and attack attribution. By correlating multi-layered IDS outputs, one can detect patterns of behavior that may indicate a modus operandi. This can be useful in tracing the sources of unwanted behavior. The correlated outputs of host- and network-based IDS at various levels can also be used to direct attention to potential threats. Resources such as human system administrators and various intelligence assets can be directed in this way. The use of a PKI and PK-enabled applications can greatly reduce the noise level of amateur attacks coming into the GIG, and thus increase the signal to noise ratio of the existing indicators and warnings in the GIG.

Fine-grained access control (FGAC) is the principle that allows access to computing and communication resources to be shared, in a safe manner, among a large number of users and user communities. Technology is available to enforce FGAC with an acceptable level of computational overhead, but tools must be available to enable local administrators and users to efficiently manage FGAC for WANs, LANs, and individual hosts and servers.

Accountability is supportive of FGAC and acts as a deterrent to inside attacks. Fine-grained identification and authentication, i.e., via use of level-4 PKI, provides the inputs needed to make FGAC decisions. Intrusion detection mechanisms help detect attacks that have eluded access controls, or activities that represent inappropriate use of resources by authorized personnel.

GIG IA/SA Strategies (concluded)

- Establish DoD-wide IA testbed
 - ❖ Use “nation-state-level” technical red team
 - ❖ Tightly integrate blue team
 - ❖ Transition lessons learned to operational GIG
- Qualify suppliers
 - ❖ Use commercial service level agreements, warranties
 - ❖ Ensure standards compliance
 - ❖ Assess vendor response to bug fixes
 - ❖ Use IA testbed to continuously test, evaluate, and improve
- Focus R&D investment
 - ❖ Develop countermeasures in anticipation of attacks
 - ❖ Intrusion tolerant systems (e.g., self healing)
 - ❖ Security for mobile code
 - ❖ IA forensic technologies

Figure 31. GIG IA Strategies Concluded

The fifth strategy is to establish a DoD-wide GIG IA testbed. This testbed would draw blue team members and current configuration information from GIG operations, and employ a nation-state-level technical red team. The lessons learned through these exercises should be used to upgrade the IA properties of the testbed, and if successful in defense, should be transitioned to the operational GIG. Building an IA testbed avoids the costs and other issues inherent in red-teaming the live operational GIG.

A sixth strategy is to more stringently qualify suppliers of GIG IA technologies than is current practice in government procurement. It is imperative that the DoD becomes a smart buyer of commercial information and information assurance technology and services. Commercial information services can often be bought with service level agreements (SLAs) and/or warranties. SLAs can cover a variety of service aspects. For example, an SLA for a communications service might cover: 1) communication speed, 2) link availability, and 3) notifying the customer within certain timelines of problems. In the future, we expect that SLAs may also address security issues.

It is also important to assess suppliers' conformance with applicable standards. There are numerous organizations that measure and certify compliance with a wide range of standards, such as Underwriter's Laboratory. In the information security area, conformance with the Common Criteria, evaluated under the auspices of the National Information Assurance Partnership (NIAP) is particularly important. The NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The NIAP encourages the development of commercial products with security features as specified in

the Common Criteria, and certifies commercial laboratories to evaluate products against the criteria under NIST's National Voluntary Laboratory Accreditation Program (NVLAP). In implementing the GIG, strong preference should be given to products evaluated under the NIAP.

Another way to qualify suppliers is to gauge their commitment to fixing security-related flaws found in their systems. There are numerous organizations that compile information about vulnerabilities in commercial systems, among them the CERT at Carnegie-Mellon University (www.cert.org), the SANS Institute (www.sans.org), Security Focus (SecurityFocus.com), and NTBugtraq (www.ntbugtraq.com). In implementing the GIG, strong preference should be given to suppliers who have a track record of quickly fixing reported flaws. Furthermore, preference should be given to products that are compatible with the Common Vulnerabilities and Exposures (CVE) list. CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools with a "common enumeration."

Furthermore, while the vulnerabilities of commercial technology need to be understood, the impact on the overall GIG architecture of adding the technology needs to be weighed before employment. We recommend that the GIG IA testbed be used to address this issue. As mentioned above, there is a great deal of publicly available information about technology and product vulnerabilities. The testbed should use this information as a starting point for developing a knowledge base of technology and product benefits and vulnerabilities.

The DoD should develop a deep understanding of how commercial services are provided, so that they can be properly specified when purchased. For example, buying communication lines from multiple suppliers in order to gain redundancy and diversity may not yield the desired results, if each supplier's fiber goes through the same physical switch or runs over the same physical bridge. Instead, when buying a second communication line, DoD should specify that the line share no physical components or transit mechanisms with the first communication line.

The final strategy recommended is to adequately resource a focused GIG IA R&D program. Current DoD IA R&D does not adequately address the IA needs of the GIG. Countermeasures must be developed in anticipation of attacks. The GIG IA testbed the panel recommends can be used to experiment with potential fixes before any form of specific attacks are found live on the GIG. The development of self-healing systems that are intrusion-tolerant and fault-tolerant is an important step in deploying a reliable GIG infrastructure. Self-healing, recovery, and reconstitution of GIG components could provide continuity of operation throughout and after significant attacks. Clear commercial trends point toward mobile code as an increasingly important software distribution and maintenance mechanism. Current practices in some networks of stripping mobile code out of incoming e-mail and disabling Java and JavaScript are stopgap maneuvers. Significant focused research is called for to contain and verify mobile code, to discover new methods of utilizing mobile code to defend against attacks (i.e., throttling incoming traffic at the routers during a denial-of-service attack), and to automatically install 'good' viruses that upgrade system survivability. R&D focused on forensics, tagging, and traceback could provide GIG administrators with the tools necessary to trace attacks back to their source. Non-repudiable identification of malicious attackers and wayward insiders can provide a level of deterrence not currently in evidence.

4.3 DEFENSE-IN-DEPTH

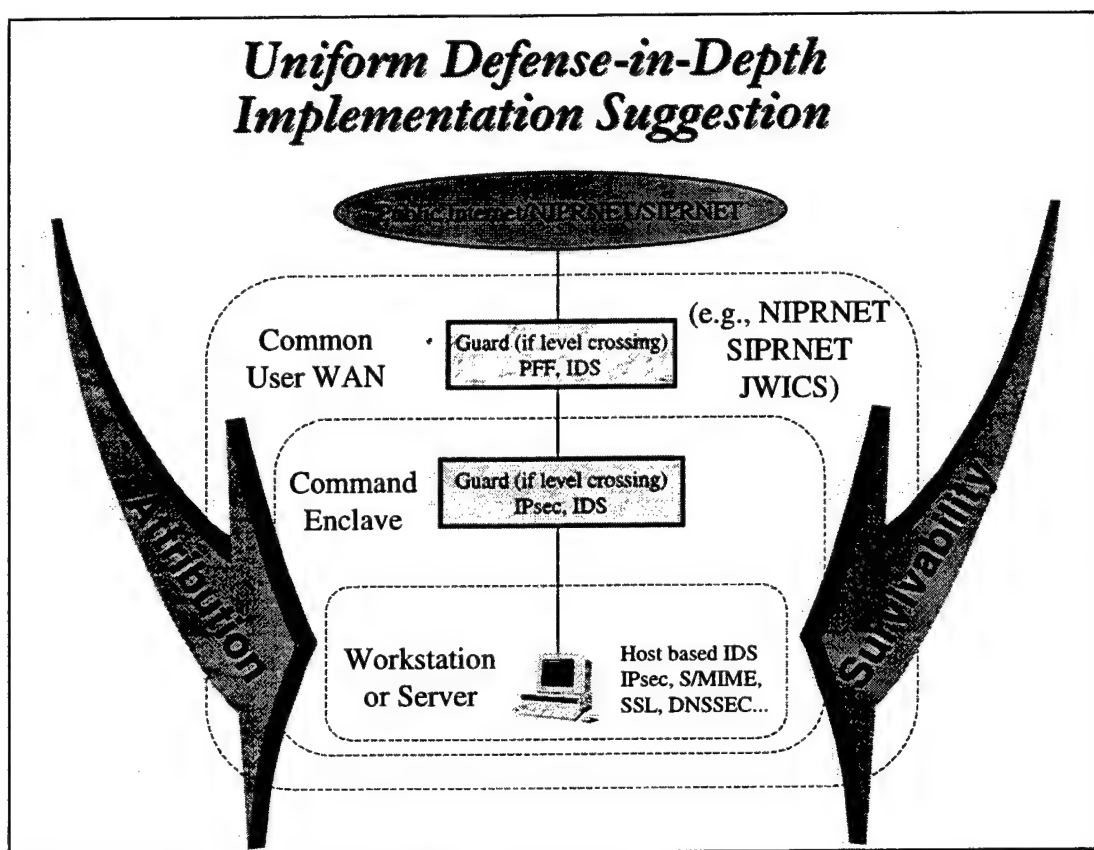


Figure 32. Uniform Defense-in-Depth Implementation

Figure 32 provides an example of layered defense, or defense-in-depth, from a traffic flow perspective. *All* DoD common user networks, SIPRNET and JWICS as well as NIPRNET, should reflect this architecture. This is a departure from current practice in which the classified networks do not provide significant barriers to attacks launched from sites in the same community, i.e., other subscribers to the same common user network.

The outer perimeter represents an interface between a single-level, common user WAN, i.e., NIPRNET, SIPRNET, or JWICS, and a less sensitive WAN, i.e., the public Internet. (If a sensitivity level is crossed, i.e., from SIPRNET to NIPRNET, then a guard is employed.) This perimeter is protected by the use of a (stateful) packet filtering firewall (PFF) and an IDS. Non-IPsec or SSL protected traffic, i.e., e-mail, DNS, and web traffic, is screened via the PFF, and restricted to destinations inside the WAN that are well-defined web servers, e-mail servers, etc. The IDS here is used to screen traffic (at very high data rates) to detect patterns of attacks against multiple sites on the WAN, through correlation of analytic data from each of these IDS systems. Virus scanning might even be applied to (non-encrypted) e-mail attachments at this point, via the use of implicit mail relays.

At the enclave boundary, IPsec is the primary defense mechanism, preventing unauthenticated connectivity to external sources. A PFF is used for traffic that would not be afforded IPsec protection, i.e., e-mail and DNS services. (As illustrated in later discussion, web data designed to be available for public access will be maintained outside of the enclave boundary.) The enclave IDS has access to some plaintext data (except when IPsec or SSL is used all the way to a workstation or server) and thus can perform more analysis than the WAN IDS. Virus scanning can be applied to (non-encrypted) e-mail attachments at this point, if it is not applied at the WAN boundary.

Each workstation or server is equipped with an IDS, which is monitored by the enclave security administrator. IPsec, SSL, and S/MIME are available for end-to-end cryptographic security, including authentication, integrity, confidentiality, and access control. A secure DNS resolver interacts with secure DNS servers.

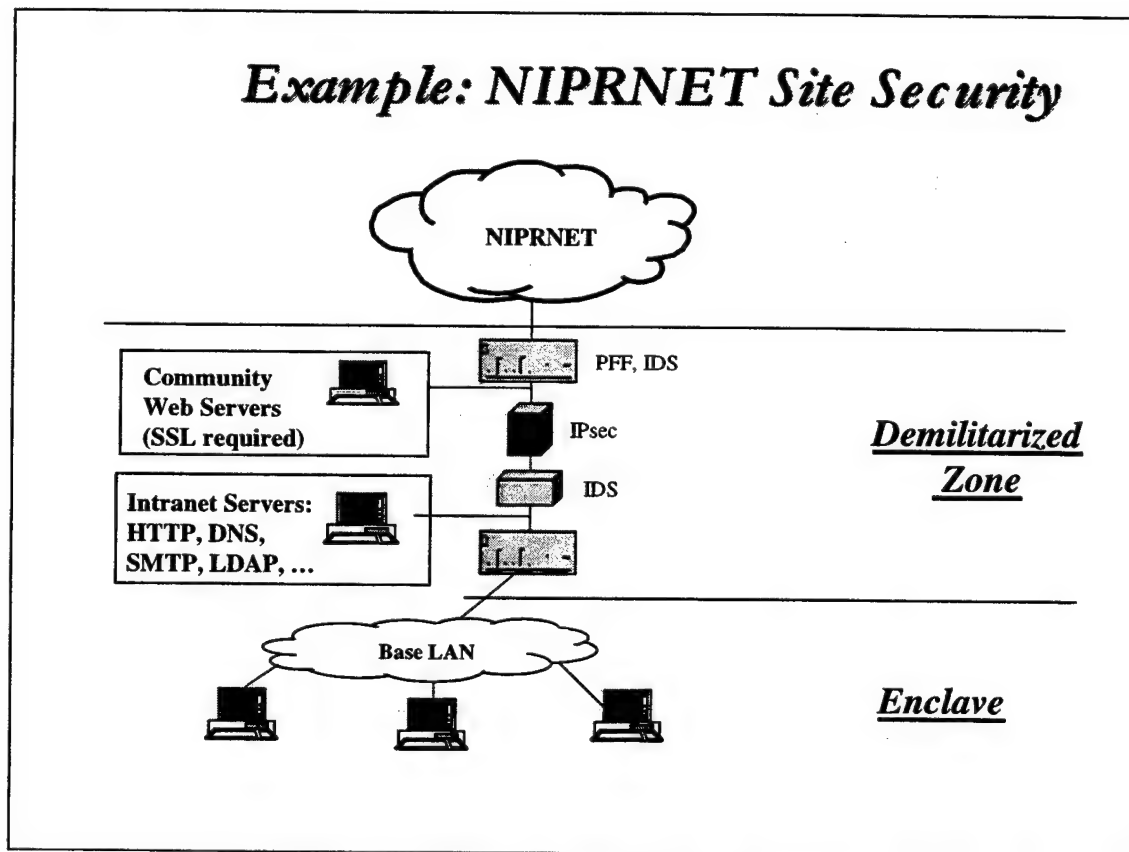


Figure 33. Example: NIPRNET Site Security

Figure 33 illustrates the IA components that would be employed at the interface to a typical NIPRNET site to implement the panel's suggested defense-in-depth architecture. The Packet Filter Firewall (PFF) at the attachment point to the NIPRNET filters out traffic that should never access the web server. The IPsec device in the DMZ is the primary access control mechanism. It implements a basic PFF, as required by the IPsec specifications (RFC 2401). This device, or one immediately behind it, incorporates an IDS that focuses on non-encrypted traffic that traverses

the IPsec device. Examples of such traffic include transport mode IPsec or SSL traffic destined for machines on the base LAN. (Note, S/MIME protected mail cannot be scanned for viruses at the SMTP server, but any e-mail with viral attachments can be tracked to its sender when S/MIME has been used. This provides reliable attribution of such e-mail, which acts as a deterrent and provides excellent forensics. The host-based IDS will examine incoming e-mail attachments for malicious code upon receipt and decryption.)

The DMZ IDS monitors traffic that bypasses the IPsec device (i.e., DNS traffic or SMTP traffic from the Internet) as well as decrypted traffic from other NIPRNET sites and from contractor sites. (A LAN-based approach may also be employed if technology permits.)

The servers behind the IPsec device are accessed via a mix of plaintext and crypto-protected traffic streams. For example, DNSSEC and e-mail protection is at the application layer, whereas LDAP traffic may be unauthenticated or may be SSL/TLS protected. The latter will be required for access to sensitive directory entries and for all infrastructure management functions.

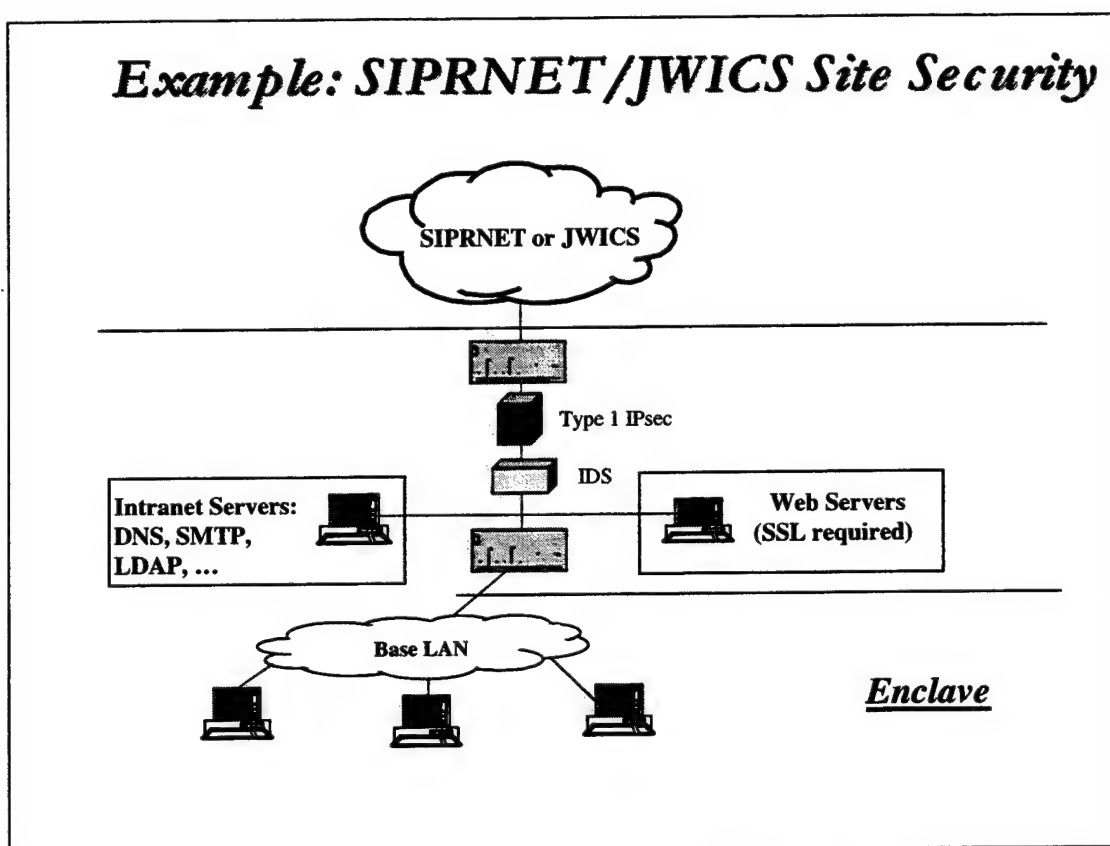


Figure 34. Example: SIPRNET/JWICS Site Security

Figure 34 is similar to the NIPRNET example. Note that there are no DMZ community servers, because all traffic is IPsec protected. This approach is feasible because there is no direct communication with sites not on the same, common user WAN. All sites on SIPRNET or JWICS will be equipped with Type 1 IPsec devices and thus all traffic entering or leaving a site is protected and subject to access controls.

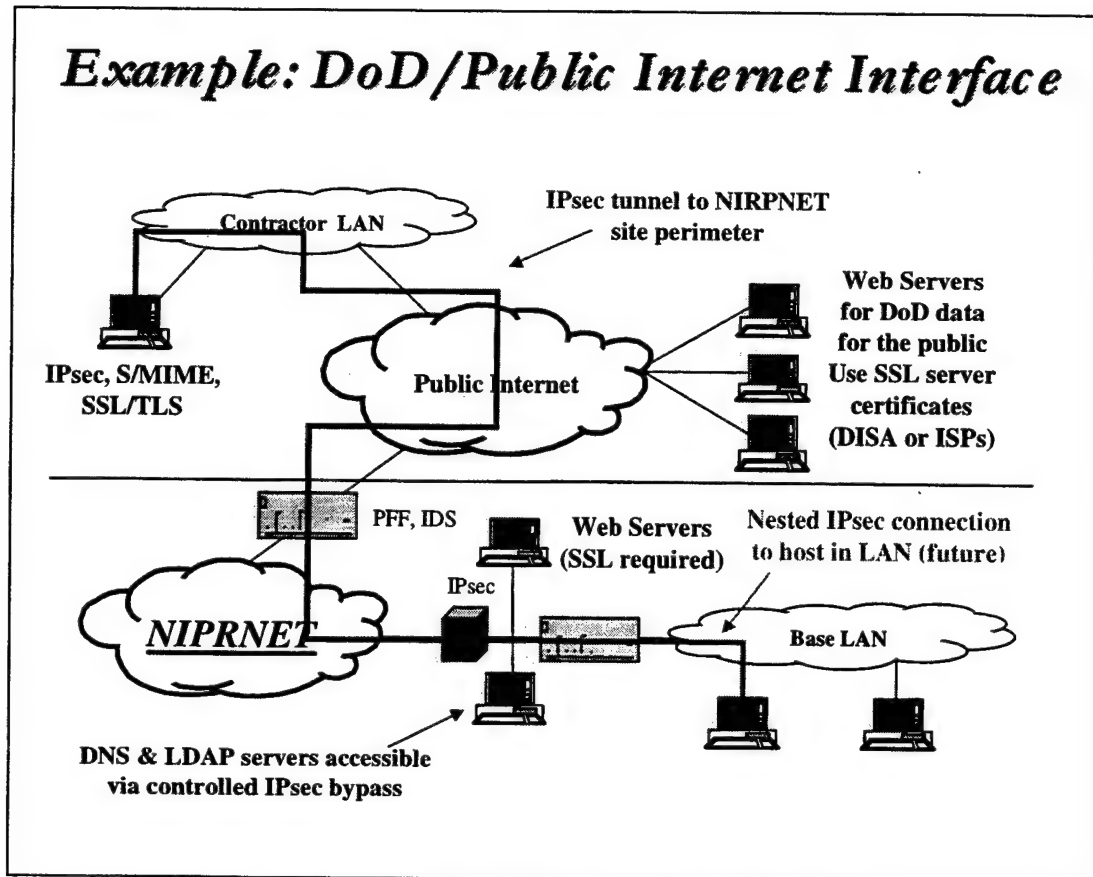


Figure 35. DoD/Public Internet Interface

Figure 35 illustrates the suggested interface between NIPRNET sites and the public Internet. In this approach, all DoD data that is releasable to the general public should be housed on web servers that *are outside of* NIPRNET. This segregation keeps traffic associated with this data off of NIPRNET, avoiding potential congestion on NIPRNET due to “legitimate” access. It also minimizes opportunities for denial-of-service attacks against NIPRNET that masquerade as legitimate access to public Web pages. The web servers holding this data could be operated by DISA on behalf of all DoD activities, or could be outsourced to commercial providers, i.e., ISPs.

Contractors, universities performing DoD sponsored R&D, and other users authorized to access resources on NIPRNET must use secure protocols and employ individual certificates. For example, access to a web server at a NIPRNET site will require SSL/TLS, with client certificates. E-mail will be protected using S/MIME. The assumption is that each organization will establish a PKI and issue certificates to its employees in order to support these security protocols.

These requirements seem quite feasible. SSL/TLS is integrated into freely available browsers. IPsec is built into Windows 2000 and should soon be available in Sun OS and Linux. (After-market IPsec implementations are available for Windows 95 and 98.) Access to web servers behind the enclave IPsec device makes use of SSL, which is bypassed by the IPsec device (when the destination is one of a set of selected web server at the site). Most IPsec traffic to a site will terminate at the IPsec device, which enables local IDS examination of the traffic. However, a site

may authorize nested IPsec traffic for true end-to-end security where appropriate. S/MIME e-mail (with triple wrapping) from approved sources is protected all the way to the recipient, while other e-mail is subject to scrutiny at the SMTP server, i.e., attachments will be scanned for viruses and some types of attachments may be prohibited.

Many organizations have, or have plans to establish their own PKIs. Small scale CAs are either free, i.e., Windows 2000, or inexpensive, i.e., the Netscape Certificate Server (which costs about \$1,000). The major costs of instituting an organizational (local) PKI are administrative, not capital. Thus it does not seem unreasonable to mandate that organizations doing business with the DoD establish a PKI for secure communication purposes. (The DFAR might explicitly authorize some of the costs of PKI establishment and maintenance as chargeable to DoD contracts.)

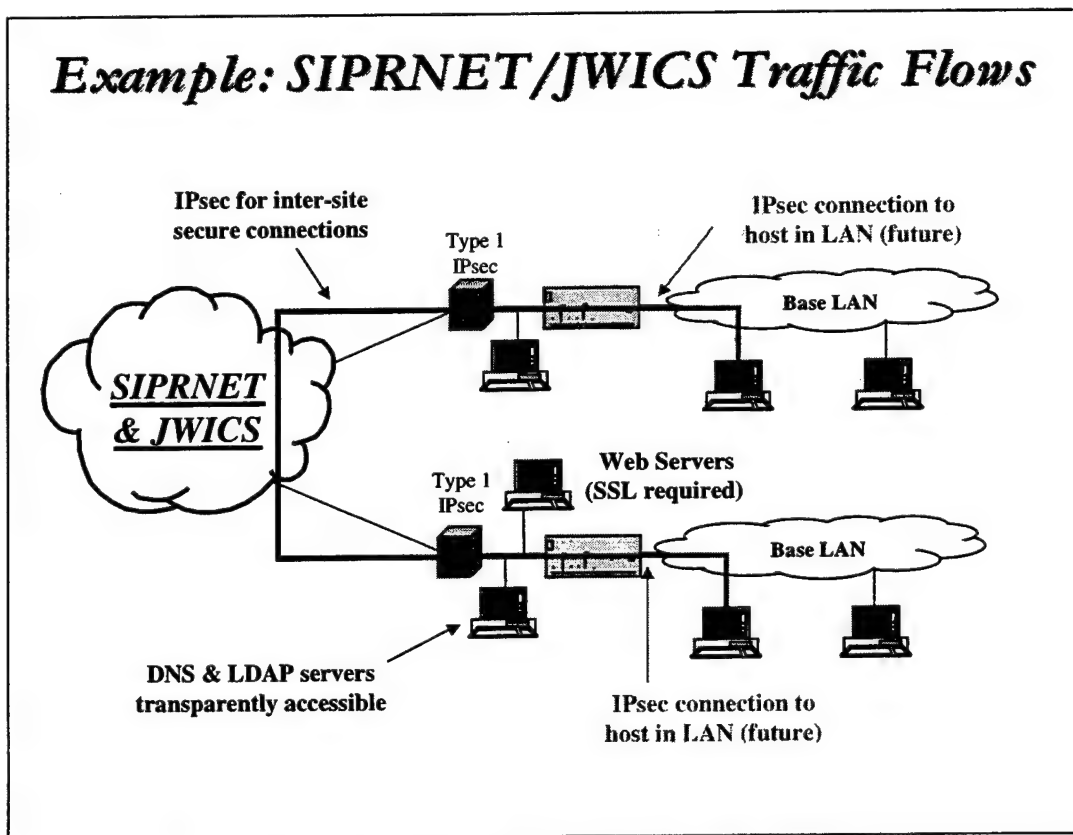


Figure 36. SIPRNET/JWICS Traffic Flows

Figure 36 illustrates connections between users or between a user and server at two SIPRNET or JWICS sites. The Type 1 IPsec devices at the perimeter of each enclave provide confidentiality, authentication, integrity, and access control for all traffic, transparently. Because all inter-enclave traffic is protected by these devices there is not need to bypass traffic. (Special provisions may be required for dual-homed enclaves that need to exchange BGP traffic with routers in the SIPRNET or JWICS backbone.) Thus all servers, including e-mail, DNS, and web servers are "behind" these devices. Each site is responsible for managing the access control lists in the Type 1 IPsec device(s) at its enclave boundary.

When a user in one enclave needs to send or receive data to or from a computer in another enclave, if further protection is required (in support of FGAC), IPsec, SSL/TLS, or S/MIME is employed. For example, all web server access is SSL/TLS protected. S/MIME is used to protect all e-mail. IPsec is employed when accessing other systems where SSL/TLS is not appropriate, i.e., where UDP (vs. TCP) is employed for transport.

Guards, which provide controlled upgrade/downgrade connectivity to networks at different sensitivity levels, are located in enclaves, and thus communication with them follows this same paradigm.

Suggested IA Functions in the Host

- Host-based intrusion detection and response
 - ❖ Attack signature detection
 - ❖ Anomaly detection
- End-to-end security
 - ❖ IPsec trust termination
 - ❖ S/MIME
 - ❖ SSL
- DNSSEC
 - ❖ High assurance domain name resolution
- Malicious and mobile code eradication
 - ❖ Virus detector
 - ❖ Malicious code scanner
 - ❖ Mobile code filter

Figure 37. Suggested IA Functions in the Host

In addition to boundary protection provided by the DiD architecture, there are a variety of functions that should be employed to defend the hosts in the GIG. The panel suggests that these be used in all DoD common-user networks, including NIPRNET, SIPRNET, and JWICS.

IPsec, SSL, and S/MIME should be used for end-to-end cryptographic services such as confidentiality, authentication, nonrepudiation, integrity, and access control. A secure DNS resolver should be deployed with secure DNS servers to provide high assurance that a domain name is resolved correctly. A virus scanner, malicious code detector, and mobile code filter should be used to strip any attachments or content violating mobile code policies established within an enclave.

In keeping with the defense-in-depth strategy, host-based intrusion detection and anomaly detection tools should also be deployed. When IPsec is used all the way to the host, the host has the only opportunity to apply serious IDS scrutiny to incoming packets. Since the hosts will experience relatively small data rates, the IDS can be tuned to high levels of sensitivity. The host-based IDS should communicate alert information to other enclave IDS services which can correlate data from network IDS and other host-based IDS deployed in the enclave to obtain a more accurate enclave-wide view of intrusive and other network activity. Signature-based IDS should be kept up-to-date and output monitored by the enclave security administrator.

Suggested Secure Net Management

- Network components require secure, remote management capabilities
- SNMP & Telnet are widely used for management today
 - ❖ Not secure
- SNMP v3 security is not PKI-enabled
 - ❖ A commercial-sector focus
- Suggestions:
 - ❖ Use Kerberos v5 (or TLS) with SNMP & Telnet
 - ❖ Use PKI-enabled link crypto (e.g., STE) for physical layer switch management

Figure 38. Suggested Secure Net Management

Today, most layer 3 and above network components are managed remotely using a mix of SNMP and Telnet, although some offer web interfaces as well. Simple Network Management Protocol (SNMP) v1 offered no security, and so was used only for getting information from managed devices (for reading MIBs, but not for modifying them). Telnet, even if used with plaintext, reused passwords, was often employed. SNMP v2 had static, symmetric key cryptographic security added, but was not commercially successful. SNMP v3 has improved security services, but still uses manually distributed, symmetric keys. This is not consistent with our proposed use of PKI for user authentication and authorization everywhere else in the GIG. The use of Kerberos for SNMP v3 security has recently been proposed. Version 5 of Kerberos supports X.509 certificates and thus may provide a means of PKI-enabling SNMP v3.

Telnet, secured by Kerberos, is available and used today in some products for secure SETs, and web interfaces for management can make direct use of SSL/TLS. Telnet can also be secured using SSL/TLS.

For the most part, the GIG will not own or directly manage circuits, but when it does, the circuit switches, SONET switches, and the like often require or offer out-of-band management interfaces, i.e., via the PSTN. These interfaces should be secured via link crypto devices that make use of PKI technology, to provide authenticated, integrity-protected, and confidentiality-secure channels. Some such devices are commercially available, and one can use STU-IIIs (or, preferably, the next generation technology, STEs) in this fashion as well.

Suggested DoD PKI Strategy

- DoD must own and manage its own PKI
- DoD must deploy level 4 PKI as a top priority
- DoD PKI should be organizationally aligned, to ensure accountability, and minimize risks associated with errors and attacks
- NSA's Key Management Infrastructure (KMI) must provide
 - ❖ Unified ordering interface for users
 - ❖ External interfaces to non-DoD CAs
 - ❖ High level of assurance

Figure 39. Suggested DoD PKI Strategy

As suggested in Figure 39, DoD should focus on deployment of level 4 PKI. If this requires delaying Common Access Card (CAC) deployment that delay should be tolerated. A PKI is a central element of system security and subversion of a PKI can undermine most layers of a defense-in-depth scheme. Thus it is critical that DoD take responsibility for its own PKIs. The DoD should *not* make use of commercial CAs, although the DoD PKIs must interoperate with commercial PKIs, i.e., to support authentication of DoD contractors.

The DoD PKI should be aligned with organizational boundaries and should use alternate (subject/issuer) name extensions to incorporate DNS names and RFC822 names in order to facilitate native support of security protocols such as S/MIME, IPsec, and SSL/TLS. The NSA

key management infrastructure (KMI) could provide a suitable infrastructure for these requirements. It is critical that certificates be issued along organizational boundaries, to constrain the damage that might result from local security compromises. For example, it must not be possible for an Army CA to issue a certificate that purports to be for an Air Force employee. Current plans for the KMI do not necessarily adhere to this principle and should be modified accordingly. Also troubling is the so-called "bridge CA" concept, developed for inter-organizational cross certification in the federal PKI. Several important PKI security features do not operate properly when a bridge CA is part of a certification path. A bridge CA should be used *only* to facilitate acquisition of public key certificates of other organizations, so that local security administrators can issue cross certificates directly to the other organizations with which they need to interoperate.

DNSSEC is a PKI-like system that provides secure name/address translation support for most Internet protocols. The DNS is global in scope and thus the DoD should encourage widespread adoption of DNSSEC. Within the DoD, high assurance (cryptographic) technology should be employed to protect DoD domains, i.e., the DoD should implement DNSSEC for the .mil and .sml domain and sub-domains.

Directories are essential for widespread deployment of e-mail security (S/MIME), because a sender must retrieve the certificate for a recipient prior to encrypting a message. IPsec and TLS do not rely on directories, except for certificate revocation status information. LDAP is the current, commercial directory interface standard; it is a rapidly evolving standard, of growing complexity. Security for directory access, i.e., via TLS, is improving, but implementations will probably remain significantly vulnerable for some time. The DoD must ensure that the directory systems it deploys make use of the best available load sharing, replication, and security.

Countering the Insider Threat and Providing Survivability

- Suggested Systems Architecture addresses insider attacks via:
 - ❖ Use of IDS's to detect anomalous behavior (including insiders)
 - ❖ Use of IPsec, SSL/TLS, and S/MIME to provide intranet & extranet confidentiality for traffic
 - ❖ Use of IPsec and SSL/TLS for intranet & extranet access control
- Systems Architecture addresses survivability via
 - ❖ Spatial, temporal, and information redundancy
 - ❖ Design diversity (vs. monoculture)
 - ❖ Reconfigurability

Figure 40. Countering the Insider Threat and Providing Survivability

The panel's suggested system architecture and DiD address the insider threat previously discussed. Intrusion detection systems deployed in enclaves, on user workstations servers and other devices, monitor activity to detect inappropriate (i.e., suspicious) behavior by authorized personnel, as well as attacks by outsiders, which should provide a deterrent to some class of insiders, as well as aid counter-intelligence efforts.

The security protocols cited above (IPsec, SSL/TLS, and S/MIME, level-4 PKI) support fine-grained access control to information in storage on servers and in transit. This fine-grained access control helps prevent a subverted insider from eavesdropping on communications inside enclaves and helps prevent insiders from gaining access to servers or to other enclaves without explicit authorization. Because all of these protocols make use of PKI technology for authentication, the resulting audit trails also help to detect and deter insider misuse.

Survivability is addressed through the use of redundant servers, access lines, and local interfaces (i.e., multi-homing), and via dynamic routing in common user WANs.

Countering Denial of Service and Enabling Attribution

IA Architectural Feature	Benefits
Packet Finding Filters (PFF) and IPsec	Blocks DoS attack at edge Provide Certificate-based attribution
Nested IPsec	Provides tracking Provides locatization of target
Anomaly Detection on Military Patterns of Use	Improves response time
Content Distribution	Disperses DoS attacks Provides geographic attribution
Inline IPsec Devices	Fosters commercial robustness to DoS attacks

Figure 41. Countering Denial of Service and Enabling Attribution

In Figure 41, the panel suggests architectural elements that counter denial-of-service and provide partial ability to attribute attacks back toward their origins. The stateful packet-filtering firewalls installed at the boundaries should be configured to reject Internet Control Message Protocol (ICMP) echo and reply messages, and to throttle SYN messages to limit the number of half-open connections. Smurf attacks depend on ICMP echo reply (as well as other questionable mechanisms) that can easily be stopped at firewalls. Synchronization (SYN) floods depend on overflowing the fixed-length queues of TCP, so by throttling the number of SYNs allowed into a network, perhaps contingent on the completion of connections, one can limit the DoS potential at the firewalls.

There is a potential performance penalty associated with such throttling, but this can be managed. In the Feb 2000 distributed denial-of-service attacks, approximately 80% of the attacks were Smurf, and 15% were SYN floods. Thus approximately 95% of Feb-2000-style DoS attacks would be mitigated by present and suggested firewalls at the enclave boundaries.

The panel recommends the use of IPsec, which prevents denial-of-service within the enclaves. Further, future nested-IPsec implementations can counter denial-of-service and assist attribution by target localization and path tracking. The panel recommends research and development of networked IDS visualization tools for semi-automated sysadmin response, which would improve the time to response to a DoS attack. (It took days for sysadmins to identify the first DoS attack for what it was.) The panel also recommendation to employ anomaly detection can be configured to exploit known military patterns of use, and can trigger responses perhaps including dynamic user reauthorization. Content distribution networks, such as those run commercially by Akamai and Digital Island, provide additional mechanisms to counter DoS attacks. The static content of public DoD web sites can be replicated in a similar way. For public

DoD web sites using SSL server certificates to prevent web site defacement the current commercial offerings are inappropriate. Some content-distribution approaches provide a partial geographic attribution. Finally, the panel recommendation to support development of high-speed inline IP cryptographic device could foster widespread commercial IPsec use, initially in large multinational corporations. Together, the panel recommendations partially address denial-of-service attacks on the GIG and provide initial attribution capabilities.

4.4 METRIC SUGGESTIONS

Suggested Measures of Merit for IA

- A spectrum of metrics is necessary
- Researchers, designers, vendors, users and operators of information technology systems need metrics or measures of merit
 - ❖ R&D community needs to compare competing approaches, evaluate effectiveness of an approach on an absolute scale, and mark progress
 - ❖ Designers need to make systems engineering trade-offs
 - ❖ Vendors need to be able to certify their products, claim quantifiable advantage over competing products, and tell customers how much protection their products provide
 - ❖ Users need to evaluate competing products against their own requirements for information assurance and survivability
 - ❖ Operators need to assess the risks to their systems

An important and inadequately addressed need...
A difficult problem

Figure 42. Suggested Measures of Merit for IA

Metrics for information assurance and surveillance architectures are an important and inadequately addressed need. Researchers, designers, vendors, and operators of information systems need a broad spectrum of metrics to achieve their respective objectives. From a systems perspective there is a need to develop metrics for technical-, system-, and mission-level evaluation. This development will require collaboration amongst technical, evaluation, and operator communities. A testbed is required to provide a means for measurement of system performance given different scenarios and related information traffic. The defense-in-depth systems architecture and metrics-measuring capability facilitate new capabilities for indications

and warning. Figures 42 and 43 provide a few examples of how the metrics may be utilized by different communities at different stages of the lifecycle of a system.

The research and development community must compare competing approaches, evaluate effectiveness of an approach on an absolute scale, and mark progress as a function of time. This paradigm of common metrics, validated training, and test data has proven to be extremely successful in areas such as speech, speaker, and language recognition.

Designers need to make systems engineering trade-offs. This is particularly true when attempting to trade complexity for performance.

Vendors need to certify products, claim quantifiable advantage over competing products, and tell customers how much protection their products provide. Metrics enable an Underwriters Laboratory (UL) approach to evaluating commercial products, i.e., common data, measurements and analysis. There has been progress on this front over the last 17 years, starting with the Trusted Computer System Evaluation Criteria (TCSEC) "Orange Book," progressing to the Information Technology Security Evaluation Criteria (ITSEC), and now the Common Criteria (CC) version 2. However, there are still questions about the viability of such security evaluation criteria, as noted in the recent National Research Council report, "Trust in Cyberspace."⁷ Thus one should not expect that component evaluation will, by itself, "solve" the problems we face in engineering secure systems. Thus the approach described below, which emphasizes development of IA metrics for fielded systems, is critical.

Users need to evaluate competing products against their own requirements for information assurance and survivability. Operators need to assess the risks to their systems. Measures of merit or metrics for information assurance and survivable architectures is an important and inadequately addressed need.

⁷ Trust in Cyberspace, Committee on Information Systems Trustworthiness, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press, Washington, DC 1999, Fred B. Schneider, Editor

Suggested IA Metrics (Cont.)

The goal is to evolve a set of information assurance metrics through evaluation, measurement and analysis of system performance / resistance to attacks:

- Mission-Level
 - Task-oriented blue traffic and red team attacks
 - Mission effectiveness (mission specific parameters) i.e., time-to-complete, targeting, losses, situation awareness accuracy
- System-Level
 - Availability
 - Response-time to neutralize attack
 - Time to reconstitute / repair damage
 - Percentage of successful attacks
 - C² information latency
- Technical / Component-level
 - P_D vs. PF_A (intrusion detection)
 - Lost packets
 - Data integrity

The need to develop metrics for technical-, system-, and mission-level evaluation will require collaboration amongst technical, evaluation, and operator communities

Figure 43. Suggested IA Metrics

The overall challenge, based on the architectural environment and an evolutionary experiment, evaluation, and analysis process, is to develop a set of information assurance metrics to measure system performance in the face of a wide-ranging set of attacks. At the mission-level, the metrics will involve task-oriented blue team operations and traffic and red team attacks to evaluate overall mission effectiveness. Mission level metrics would cover such topics as time-to-complete, targeting success, losses, situation awareness, timelines and accuracy, etc. Systems-level metrics are related to mission-level metrics but are finer grained and would cover overall system availability; response time to neutralize attacks, reconstitute and repair damage; percentage of successful attacks; and C2 information latency. At the technical and component level, suggested metrics include specific measurements of probability of intrusion detection vs. false alarms, to provide a basis for performance quantification. In addition, measurements of packet loss and data integrity and losses will provide a means for evaluating the overall performance of information systems. The relationship of measurements and performance at all levels will require collaboration amongst the technical, evaluation and operator communities.

Test, Evaluate, Improve IA and IA Metrics

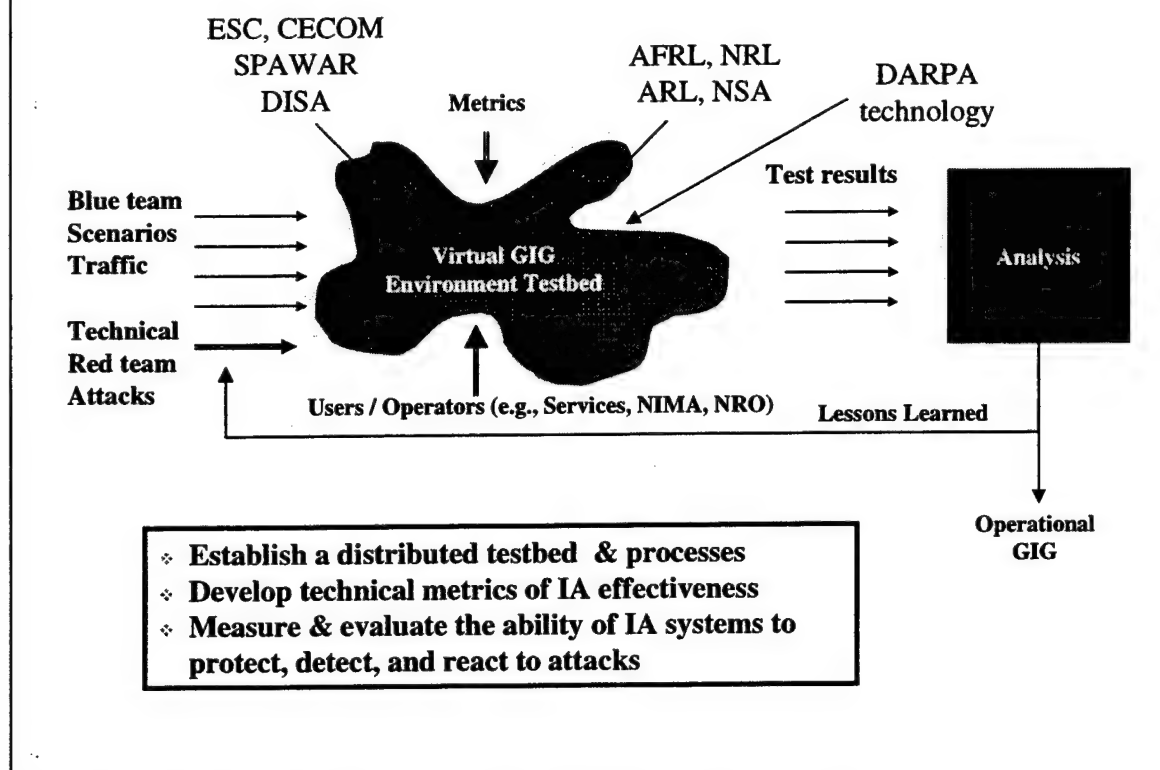


Figure 44. Test, Evaluate, Improve IA

The goal of information assurance metrics is to evaluate the ability of information assurance systems to protect, detect and react to attacks. As noted in Figure 44, to achieve this goal it will be necessary to establish a distributed testbed and processes for developing information assurance effectiveness metrics. Testbed nodes should be located at the U.S. Air Force Electronic Systems Center (ESC), U.S. Army Communications Electronics Command (CECOM), Space and Naval Warfare Systems Command (SPAWAR), Air Force Research Laboratory (AFRL), NSA, etc. The participants in the evaluation process will include research and development, evaluation, and operational communities (services and agencies). The testbed will provide a means for measurement of system performance in the face of red team attacks on blue team scenarios and related information traffic. The testbed will also serve as a primary means for DARPA information assurance technology insertion and evaluation. The metrics and measurements will evolve as results are analyzed and lessons learned are derived from the data. Lessons learned will be fed back to red and blue teams to refine and update strategies and will be used by developers to improve system defenses. Lessons learned will also be made available to the GIG architects and system engineers to improve IA.

This evolutionary process is essential to achieving a commonly accepted basis for measuring effectiveness of information assurance systems. The overall process represents a journey rather than a destination. Change is inevitable for offense, defense, infrastructure and particularly for COTS components. Measurement and evaluation of the ability of information assurance systems

to protect, detect, and react to attacks by adversaries must track these changes to achieve continued protection.

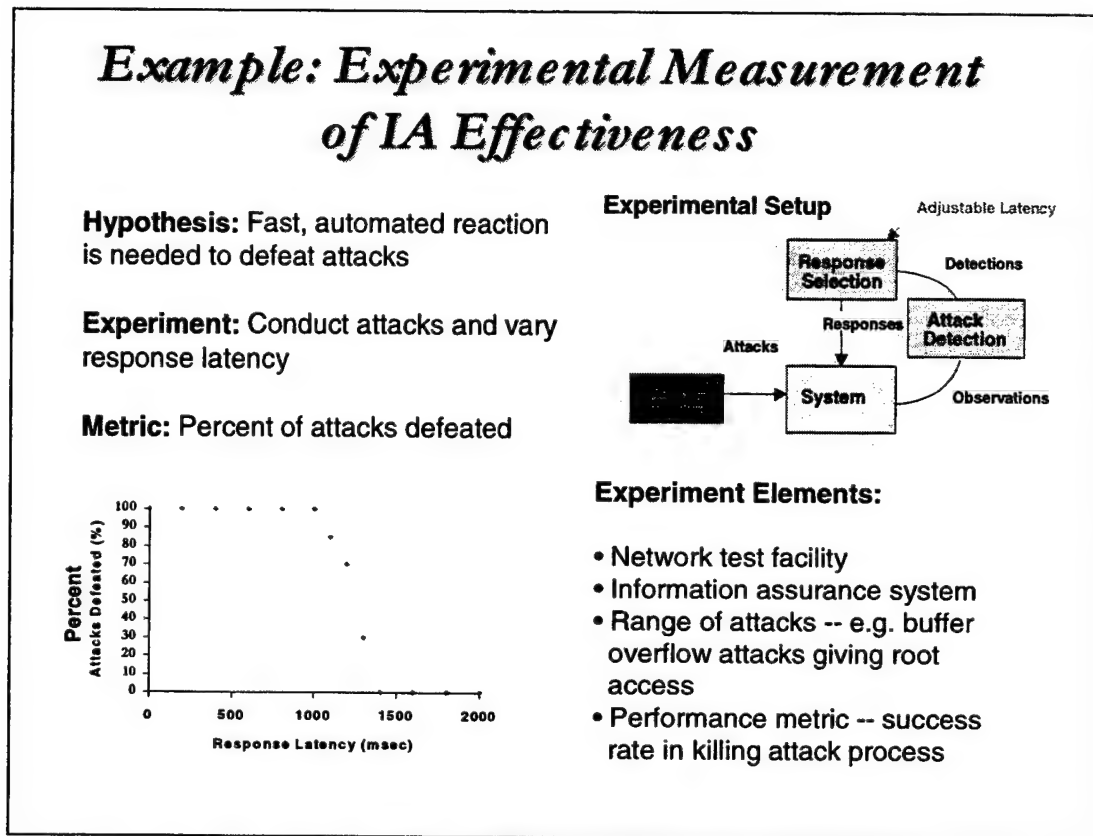


Figure 45. Example: Experimental Measurement of IA Effectiveness

Figure 45 is an example of a recent experiment to measure information assurance effectiveness. In this case, an experiment team including information assurance systems developers, and attack developers, was assembled to measure the effectiveness of an Information Assurance System response to detected attacks. The IA system has the capability to detect attacks and to respond in a variety of ways, i.e., by killing the attack process and removing attack scripts that may have been planted by an attacker. The latency of response time is an experimental variable – by waiting longer to respond, the IA system learns more about the attack, but might be too late to defeat the attack. The example set of attacks is built around “buffer overflow” attacks, where the attacker exploits weaknesses in the operating system to become “root,” or “superuser.”

An example of the experimental results is shown, where it is seen that a fast response (< 1 sec) defeats all attacks, while a slower response (>1.5 sec) fails to defeat any attacks. The experiment metric – percent of attacks defeated – is simple, but the experiment design, the team required, and the scenario development, illustrate the major components required for experimental measurement of information assurance effectiveness.

IA Indications and Warnings

- The defense-in-depth systems architecture and metrics measuring capability facilitate new capabilities for indications and warning
 - ❖ Intrusion detection systems:
 - ... Provide warnings at intranet, command enclave, and host level
 - ❖ IPsec Access control
 - ... Catalogs rejection of attempts to access segmented/restricted areas
 - ❖ Firewalls
 - ... Provide filtered information that can be correlated with intrusion detection systems
 - ❖ Host level/ process level indicators
 - ... Can be correlated with information from other levels

**Fusion of information from these sources provides
a powerful new means for I&W**

Figure 46. IA Indications and Warnings

As stated earlier, metrics for information assurance and survivable architectures are essential to achieving the broad spectrum of objectives of researchers, designers, vendors and operators of information systems. By implementing the defense-in-depth system architecture previously described, not only is system performance significantly improved, but a new set of system data (metrics) becomes available for indications and warning, as noted in Figure 46. The indications and warning data derive from a number of sources: 1) intrusion detection systems provide warnings at intranet, command enclave and host levels; 2) IPsec access controls provide data on illegal attempts to access segmented and restricted areas; 3) firewalls provide filtering information which can be correlated with data from intrusion detection systems; and 4) host-level and process-level indicators can be correlated with data from all of the above sources. The net result is that this multilevel, highly filtered data can be fused together to provide a powerful new means for facilitating indications and warning at multiple levels of the defense-in-depth architecture.

4.5 WIRELESS SUGGESTIONS

<i>GIG Wireless Concerns</i>	
<i><u>Why Worry</u></i>	<i><u>Potential Consequences</u></i>
<ul style="list-style-type: none">▪ No physical control of access perimeter▪ Essential to mobile tactical operations<ul style="list-style-type: none">❖ Desire to use commercial waveforms, services and equipment in theatre▪ Used in post, camp and station<ul style="list-style-type: none">❖ Provides quick insertion infrastructure▪ DoD use of commercial carriers worldwide	<ul style="list-style-type: none">▪ Interception<ul style="list-style-type: none">❖ Traffic (privacy)❖ Personnel location❖ Dialed number / packet address analysis▪ Denial of access locally▪ Denial of service system wide▪ Network disruption

Figure 47. GIG Wireless Concerns

Since before WWII, wireless facilities have been part of military operations. They have been used in radio trunking throughout the upper echelons of the force and in tactical radio nets in the lower echelons of the force. From an information assurance perspective, wireless links merit special consideration, as noted in Figure 47, because they are not confined to a physical perimeter and can be observed from as far off as space.

Recognition of wireless observability and the Soviet radio electronic combat doctrine caused these links to be both encrypted and protected against jamming. In the last twenty-five years the tactical forces have procured a wide variety of secure radio systems. Wireless facilities will continue to enable mobile military operations. Recently, efforts to “digitize” the battlespace have demanded an increased bandwidth. Increased bandwidth systems will typically have shorter ranges and thus require “ad hoc” networks to move the data around the battlefield. As a result, networked communications will move further forward in the tactical area.

Projections indicate that data will be an ever-increasing part of mobile military operations, while the level of voice information will be relatively static. Consequently it can be expected that voice and data services will ultimately be provided above a common wireless/wired tactical Internet (the GIG). Thus the security of the wireless networking is essential to the performance of

the system. In the civilian world, the use of wireless has been rapidly exploding. Mobile personal communications systems, such as terrestrial cellular services and satellite-based services, represent large economic investments. They provide ubiquitous, near-global access to the public switched telephone network from small, inexpensive user devices.

JV2020 envisions similar universal, on-the-move, information access for the military. Similarly, there are a number of emerging fixed wireless systems in use for wideband data and video access to the home. These systems are commercially attractive because they can provide service with a minimal infrastructure. For the military they can also provide "instant infrastructure" in existing and deployed post, camp and station facilities. While the use of these commercial capabilities in the GIG is attractive, these systems will be subjected to attack and, if compromised, could have system-wide impact.

Passive interception and observation of links can provide information on user location, traffic content, called party, and pattern of use. Commercial providers are incorporating some forms of privacy in their systems to prevent well publicized eavesdropping and fraud. However, network signaling information is generally available and can be used to deduce information or attack the system.

Active intervention in a wireless system, either by jamming or the use of equipment to render a system "busy," can deny access to communications service in a geographic area. More sophisticated attacks can deny particular users, or user communities, use of wireless facilities. All mobile systems depend on some system level database to allow calls to find a user. Attacks on these databases, either outright or through exploitation of fraud prevention safeguards, can disable use of worldwide wireless facilities.

Finally, as discussed subsequently the exploitation of network control structure can cause failure of the entire network. There have been examples of such failures in commercial networks due to software defects, and similar scenarios can occur due to either induced misbehavior or the use of wireless links to introduce false control signals into the network.

DoD Tactical Wireless

Protection

- TRANSEC driven spectrum spreading
 - ❖ Direct sequence
 - ❖ Frequency hopping
- Antenna steering
- COMSEC protection of information

Networking

- Tactical Internet
 - ❖ Interconnected radio nets
- Internetting
 - ❖ Extends range
 - ❖ Supports virtual nets

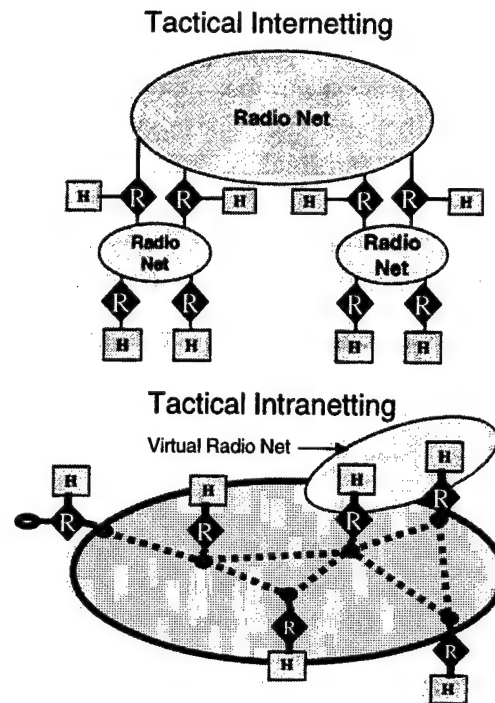


Figure 48. DoD Tactical Wireless

The DoD has led the technology development of a wide range of countermeasures to physical level attack on wireless links. These techniques may be employed individually or in concert. As noted in Figure 48, the standard technique for countering jamming is the use of spread spectrum techniques, which can be carried out with either frequency hopping or direct sequence spreading or a combination of both. The basic strategy common to both is to spread the information across a wide range of frequencies so that the jammer has to dissipate his power over the whole spectrum, while the desired user can exploit his private spectrum access information to reject the jamming signal. Adaptive antenna arrays have also been used to spatially reject a jammer. On most tactical radio links today the information is protected by COMSEC, typically embedded in the radio.

In the forward tactical area, radio nets have traditionally served single organizations. Recently there has been a desire to move digital information across multiple radio networks to achieve wide area connectivity and coordination. Initially this has been accomplished by using routers to interconnect secured radio nets, with the routers operating on decrypted traffic (system high). The Army's interconnected system is referred to as a Tactical Internet. Various exercises have shown that the routers are vulnerable to intrusion.

With a demand for higher bandwidth and robust connectivity, the emerging system concept is to separate the radio resource from the application. In this model the radios form an intranet where each radio handles all traffic in its area. The organizational communications are then achieved as a “virtual” net – above the radio infrastructure.

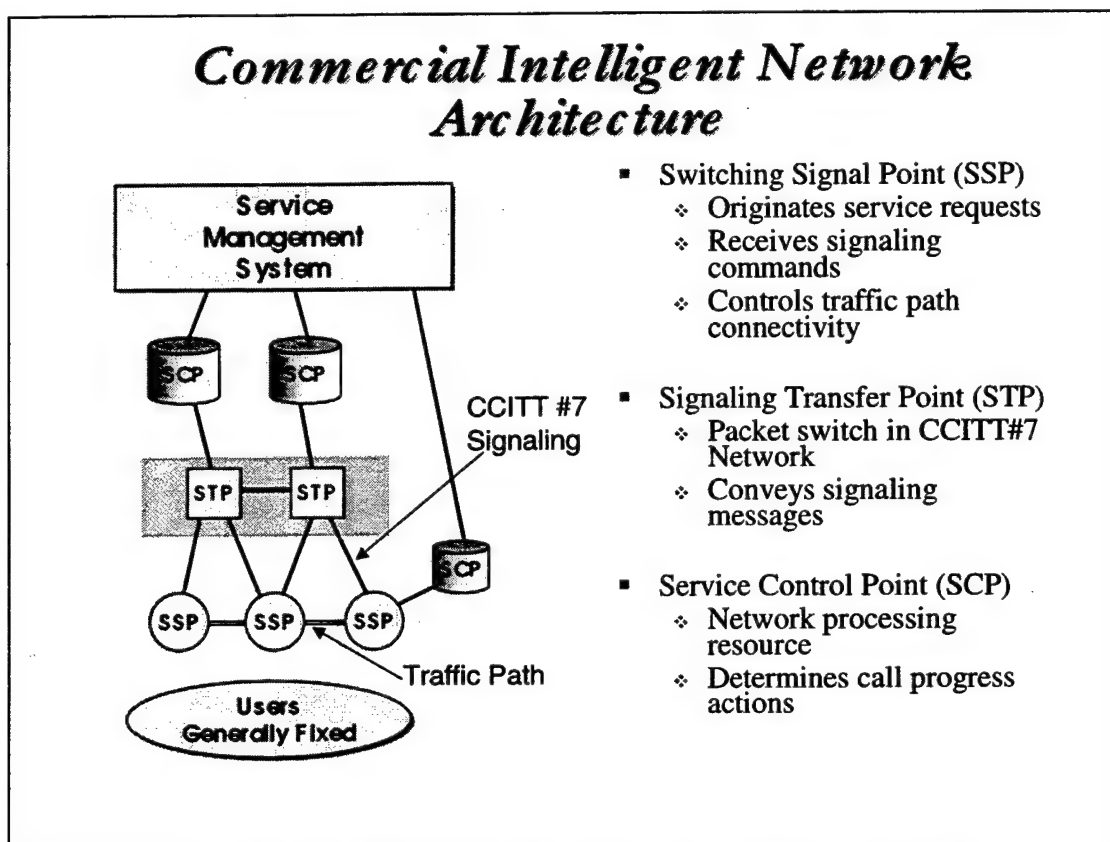


Figure 49. Commercial Intelligent Network Architecture

The GIG will use communications links in the Public Switched Telecommunications Network (PSTN). In the 80's, telecommunications providers developed and deployed a system architecture termed the “Intelligent Network” (IN) noted in Figure 49. This system architecture separated the signaling and control portions of the network from the interconnection process, so that advanced, revenue-producing, call-handling services could be provided. In this system model, a Service Switching Point (SSP) takes a subscriber's request for service and forwards messages through a network of Signal Transfer Points (STP). STPs are packet switches deployed throughout the telecommunications network. The originating SSP uses these messages to request information from Service Control Points (SCP) on how to respond to the service requests. Service Control Points (SCP) contains system-level data and processing services. In response to these requests, messages are sent to all switching points required to complete the response to the call request. The suite of protocols used to communicate these control operations has been standardized by the CCITT international standards body and is referred to as Signaling System #7 (SS7).

Access to the Signal Switching point is across an access facility. Traditionally this point has been twisted pair and considerable effort has been made to move ever-increasing data rates across this copper plant. In the 1980s, Integrated Service Digital Network (ISDN) was deployed to provide 144 kbps to subscribers. More recently, higher rates have been made available through Digital Subscriber Line (DSL) technology.

Emerging Commercial Wireless

- Mobile Personal Communications
 - ❖ Terrestrial cellular
 - ❖ Satellite (e.g., Globalstar)
 - ❖ Mobile data
- Local Multipoint Distribution (LMDS)
 - ❖ Wideband Data / video distribution to the home
- Direct Broadcast Satellite (DBS)
 - ❖ Assymetric data communications
- Satellite Wideband Internet (Teledesic, Skybridge, Spaceway, etc.)

Figure 50. Emerging Commercial Wireless

The majority of the recent wireless explosion has been in the area of wireless access to fixed infrastructure. Cellular and personal communications systems (PCS) technologies, for example, use wireless access to deliver mobile users both switched voice services and narrowband data services. Low earth-orbiting satellite systems are in the early stages of deployment. These systems allow a user access to the fixed infrastructure across a wider roaming area where terrestrial base stations may not be available. In addition, as shown in Figure 50, there are high-speed wireless access technologies, such as the Multichannel Multipoint Distribution System (MMDS) and Local Multipoint Distribution System (LMDS), whose services are based on high-bandwidth radio segments in the spectrum at the 20 GHz frequency range. Emerging wireless access methods include Direct Broadcast Satellite (DBS), which employs Ka band satellite technology to distribute entertainment programming. DBS systems also offer asymmetric, two-way data transmission supporting high-speed data transmission to the user (from the satellite system) and low-speed data reception from the user.

Wireless wide area transport systems are planned to provide low-cost, high-bandwidth data and voice service to remote areas. These systems operate from either low earth orbit (Teledesic and Skybridge) or geostationary orbit (Spaceway). Most of these systems use the 20-30 GHz band, where wide bandwidths and small antenna apertures are possible.

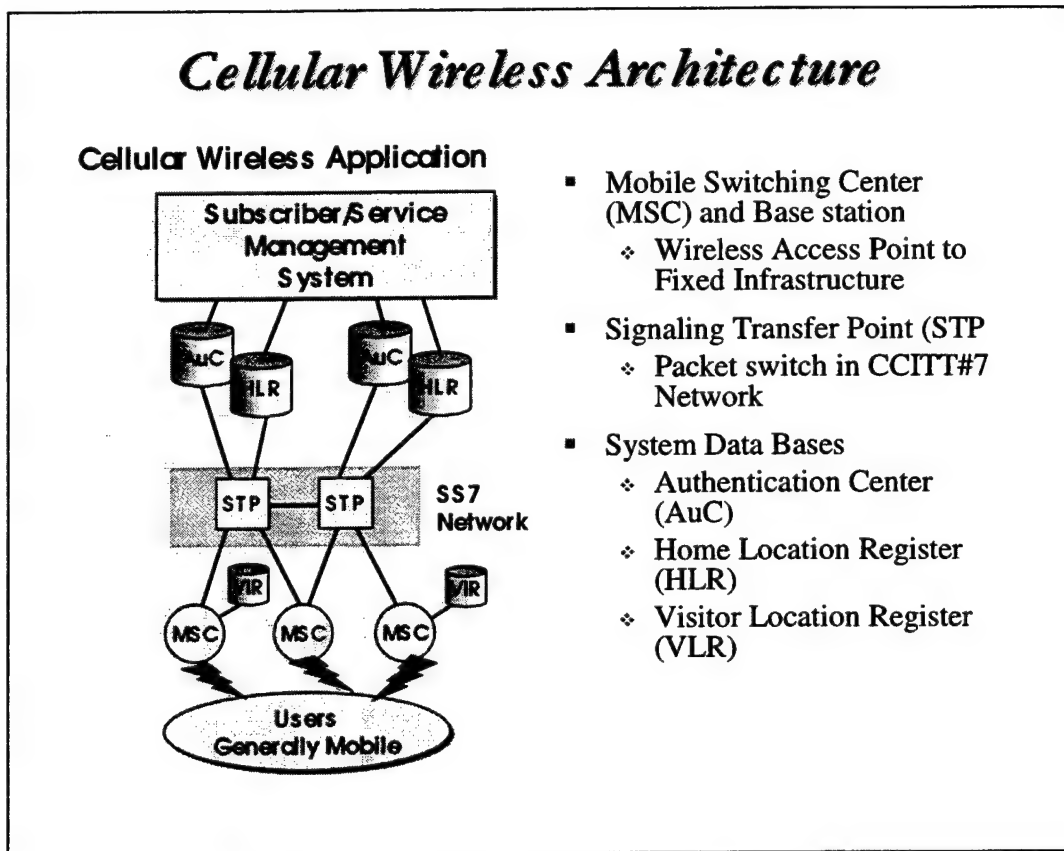


Figure 51. Cellular Wireless Architecture

The widest deployment of commercial wireless is in the mobile cellular system for which the system model is shown in Figure 51. Commercial mobile wireless services are furnished largely within the context of the Intelligent Network Architecture. The figure shows the standard wireless model. In the case of the cellular wireless application, the Mobile Switching Center serves the role of the Service Switching Point. The Mobile Switching Center and its associated Base Stations receive call requests from the mobile subscriber population. Call handling information is then requested from several key system databases, via the CC7 network. Messages are space-based on the (ANSI)-41 standard protocol suite.

These databases are: 1) the Home Location Register (HLR) which contains all of the information about the user and his current location within the system; 2) the Visitor Location Register (VLR) which contains information about all subscribers within an area served by a Mobile Switching Center (MSC); and 3) an Authentication center which validates the billing validity of the subscriber and accumulates the billing information. There may also be an Equipment Identity Center that holds information on particular devices in use within the system.

In the future, other processing resources are anticipated for new wireless-based services. One is a group of voice-controlled services, i.e., voice-controlled dialing, that allows the wireless user to control features and services through spoken commands. Another is a suite of services offering incoming-call options, where the subscriber can customize call-forwarding or call-blocking instructions for different types of incoming calls or receive calling name identification.

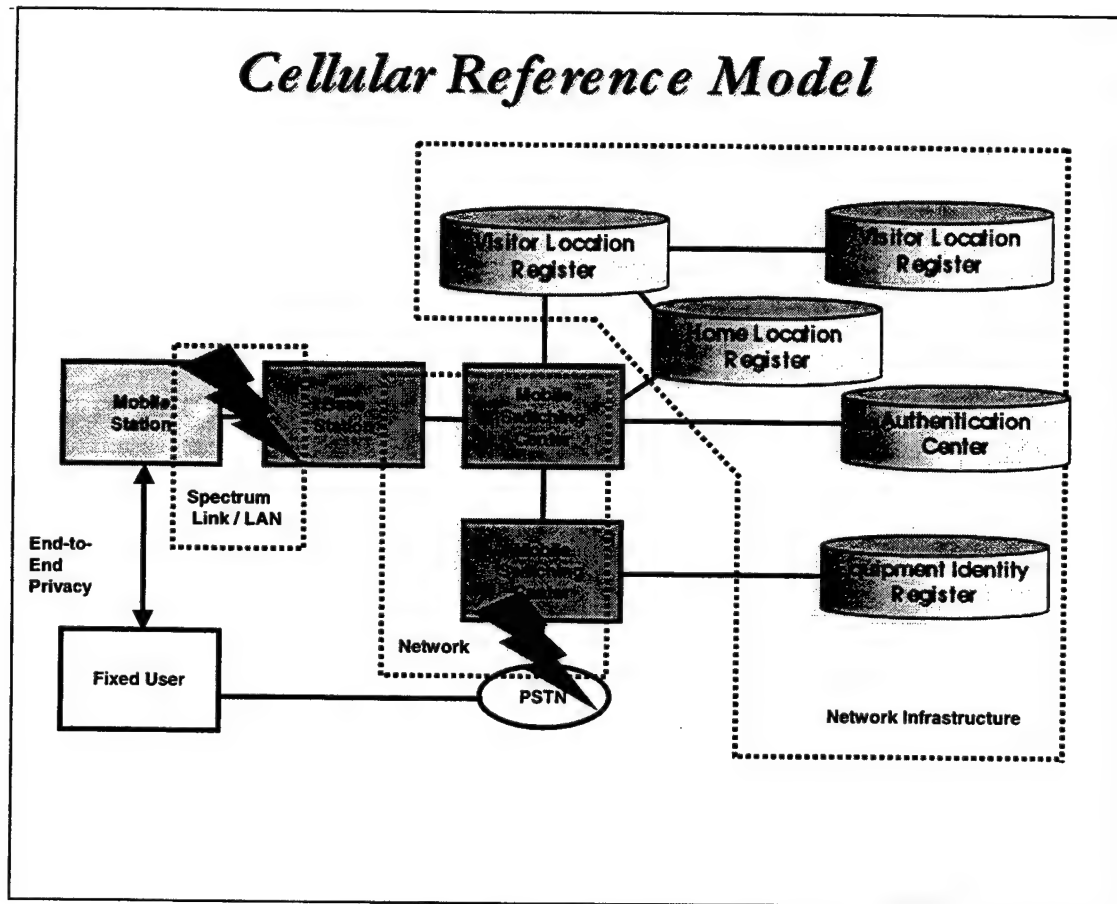


Figure 52. Cellular Reference Model

The next level of detail in the cellular communications systems model is presented in the cellular reference model shown in Figure 52. This figure illustrates the Base Station and Mobile Station that provide the subscriber access to the system. Base stations are sometimes split into one or more Base Transmission Systems (BTS) at a cell site and a Base Switching Center (BSC). Multiple BTS's can be served by a single BSC and a single Mobile Switching Center (MSC) can serve multiple BSCs.

There are several potential attack points in this system. The first is an attack on the cell spectrum or a wireless point-to-point link between a BTS and a BSC or a BSC and an MSC. The information that is accessible at this point primarily pertains to subscribers currently within the serving area of an MSC and thus has a more localized effect. Wider ranging network attacks can be mounted against wireless point-to-point links that move signaling and traffic information between system nodes, either SS7 messages to system databases or internal information such as

cell handoffs. Finally, classical cyber attacks can be mounted against any of the infrastructure databases, which are available through the SS7 network or increasingly through the Internet. While some protection mechanisms are in place, they likely will yield to a determined attack.

The key point to note is that while commercial wireless services may give the appearance of infrastructure independence, they are in truth a vulnerable extension of a vulnerable infrastructure.

<i>Utilization of Countermeasures</i>			
Threatened Area	Available Countermeasure	Military	Commercial
Spectrum Access	Waveform TRANSEC Spatial filtering	AJ LPI LPD Strong TRANSEC	Multiple Access Objective uses Weak TRANSEC Some Spatial filtering
Link	COMSEC	COMSEC – Type 1	GSM Weak
Network	IPSEC Intrusion Detection	Link Protection Only	Minimal
Infrastructure	Encryption Access Control Intrusion Detection	Access Control	Access Control
End-to-End Privacy	ETE COMSEC	Selectively	CONDOR

Figure 53. Utilization of Countermeasures

A number of countermeasures are classically available to attacks mounted at different points in the composite system, as indicated in Figure 53. Attacks in the radio frequency spectrum are the most familiar threat to the military user, and there are a variety of techniques for countering them such as random waveforms driven by high quality Transmission Security (TRANSEC) and spatial filtering of jammers by adaptive antennas. Although commercial wireless systems employ similar waveforms (GSM uses frequency hopping and IS-95 uses spread spectrum), they are designed to combat interference from other users and provide no margin against jamming. Additionally, these systems are designed for easy access.

Tactical military systems also typically protect each link with strong encryption, but only some commercial wireless systems employ any encryption, and that encryption is weak. Above the link level neither system has much protection. The tactical internet operates its routers at system high security level, while commercial systems employ rudimentary protection if any.

End-to-end Type 1 confidentiality is being provided through the NSA CONDOR program that is making commercial wireless available with embedded strong encryption.

4.6 GIG IA SUMMARY

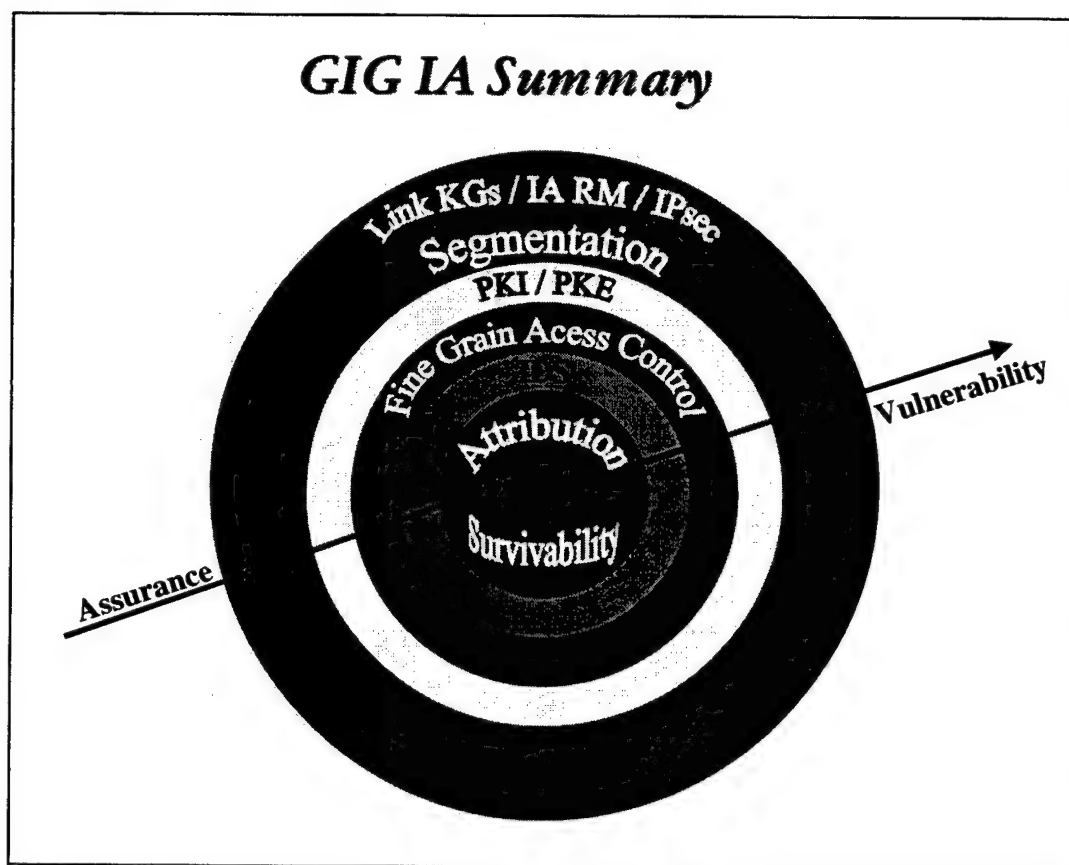


Figure 54. GIG IA Summary

Figure 54 provides a summary of the panel's suggestions for GIG IA. As we noted, the Global Information Grid is the underlying infrastructure to support information superiority for JV2020. The implementation of the GIG is one of the significant events that occurs once every decade or two. The architecture that is designed today will impact the DoD in the next decade or more. To meet this challenge, the panel has identified a layered architectural approach for providing information assurance to the GIG by pursuing a disciplined architectural approach:

- Link encryption at the physical layer
- ISO-like reference model with commercial protocols, i.e., IPsec for end to end protection

- Segmentation of DoD from Internet, and segment by classification and enclaves
- Adopt PKI/PKE
- Use fine-grained access control of computers and communication resources

In addition to the architectural layers, the approach also includes use of correlated multi-layered IDS data (i.e., at common user, command and host levels) as inputs to intelligence-enabled tracing systems and modus operandi detectors. Attribution is facilitated by highly filtered data for signal-to-noise enhancement and IPsec for path tracing and target localization. The approach of the layered defense, combined with measurement, rapid response, and attribution, results in significantly reduced vulnerability and dramatically improved GIG information assurance.

CHAPTER 5. RECOMMENDATIONS

Architecture Recommendation I

- Information Superiority Board
 - ❖ SecDef establish a DoD “Information Superiority” Board of Directors (BoD) to provide oversight and governance for the realization of DoD-wide Global Information Grid (GIG). Board to be impaneled immediately
 - Members include: Dep SecDef (chair), USD/AT&L, VCJCS, ASD/C3I
 - ❖ Board should establish an Advisory Group that draws on senior, private-sector individuals (with prior DoD experience) who are leaders in the area of internetwork technologies, commercial security technologies, emerging commercial satellite systems and the like
 - The advisory group will:
 - Bring knowledge of existing and emerging commercial technologies useful to DoD
 - Provide independent counsel to board regarding achieving the goals set in Recommendations 2 through 4
 - The advisory group should be established under federal advisory committee regulations and impaneled immediately
 - ❖ Time: 180 days from Summer Study conclusion
 - ❖ Cost: \$100,000

Figure 55. Recommendation I—Information Superiority Board

Consistent with its findings that under current organization (see discussion specifically associated with Figure 25), methods, and procedures the DoD is unlikely to realize a measured, consistent, and effective approach to creation of a Global Information Grid (GIG), the panel recommends the formation of a *DoD Board of Directors for Information Superiority*.

The Secretary of Defense should impanel the Information Superiority Board immediately, with membership consisting of the Deputy Secretary of Defense (as chair), the Undersecretary of Defense (Acquisition Technology and Logistics), the Vice-Chair of the Joint Chiefs of Staff, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director of Central Intelligence.⁸

It is further recommended that the Information Superiority Board create an advisory group under Federal Advisory Committee regulations (or as a permanent DSB Panel) consisting of senior private sector IT leaders. The Advisory Group’s purpose would be to provide the board with up-to-date knowledge of current and emerging commercial information systems, services,

⁸ Reference: Defense Science Board Report on *Tactical Battlefield Communications*, February 2000

and network technology of potential use to the DoD in the realization of its Global Information Grid. It would also offer experience-based advice from industry as to the best technical and management methods for creating such an infrastructure.

The advisory group should consist of recognized industry experts in inter-networking technologies, commercial information and network security technologies, emerging information transfer technologies and systems, and other commercial activities such as standards development, infrastructure development, and the like. The advisory group charter should also ensure that the group provides independent assessments and counsel to the Information Superiority Board concerning the achievement of the goals and objectives set forth in panel recommendations that follow.

Architecture Recommendation II

■ Implementing the GIG

- ❖ The board should establish an executive office responsible for leading and implementing the DoD-wide, common-user internetwork (transport component of GIG)

Executive director should be a minimum five year appointment and tasked to develop an implementation plan and processes, including resources to permit completion of GIG by 9/30/03

- ❖ The board should provide system engineering resources to the executive office through a dedicated system engineering team comprising 20 to 30 outstanding network systems engineers drawn from throughout DoD
- ❖ Time:
 - Office and leadership position established by 6/1/01
 - Systems engineering office and billets set up by 6/1/01
- ❖ Cost: \$10M per year

Figure 56. Recommendation II—Executive Director and GIG Implementation Process⁹

Placing the proper emphasis on GIG implementation and ensuring adherence to the policies established in accordance with the previous recommendations requires continuous oversight. It is therefore recommended that the Board of Directors for Information Superiority create, by 1 June 2001, an executive office responsible for leading the implementation of the DoD-wide common user internetwork on behalf of the board. The executive office director should be a senior DoD leader appointed for a minimum of five years. The executive director should be provided programmatic oversight for all DoD C4ISR systems acquisitions (including those procured by the services) and through this oversight ensure that all such systems are

⁹ Reference: Defense Science Board Report on *Tactical Battlefield Communications*, February 2000

interoperable within and as part of the GIG. It would be the executive director's primary responsibility to deliver the GIG.

Several additional, more specific actions needed to accomplish the GIG objectives follow:

1. The executive director should be tasked to develop a GIG implementation plan, to include technical milestones, measurable interim goals, and an estimate of the resources necessary to complete transition and realization of the GIG by 30 September 2003.
2. The board of directors should provide manpower billets for a system engineering team to support the Executive Director. A cadre of 20 to 30 outstanding system engineers with backgrounds in Internet telecommunications and security technologies should be selected from throughout DoD. These individuals must be deep technically and visionary in their system engineering skills. This system engineering team would provide independent technical inputs to the executive director regarding the many responsibilities this individual will be given, as noted in the next paragraph.
3. The executive director should immediately establish a process to transform DoD information infrastructure systems from their present stovepipe configurations into a global DoD-wide common-user virtual intranet, the GIG. This transformation must embody the current and evolving commercial IT standards, protocols, and technology, with the goal of reducing inefficiency in spectrum usage and the costs of information transport, storage, retrieval, and management. Most important, this transition should enable new operational flexibility that can be leveraged by warfighters.

Architecture Recommendation III

- Executive director should establish a consistent IA strategy for *all* GIG networks
 - ❖ Select reference model
 - ❖ Define a single system architecture
 - ❖ Address tactical & strategic systems integration issues
 - ❖ Utilize JTA security chapter as single source IA standards
 - ❖ Time: by 10/1/01
 - ❖ Cost: already included in recommendation II

Figure 57. Recommendation III—Architecture

The GIG executive director should immediately set policy and guidance for GIG IAA. Specifically, ambiguities regarding an IA reference model, system architecture, and technical architecture (as noted in the body of the IAA report) should be clarified. The executive director should establish this unified strategy and framework no later than October 2001.

Architecture Recommendation IV

- Executive director should implement the system architecture through DoD CIO and Service CIOs
 - ❖ Continue to aggressively deploy PKI, address scalability issues
 - ❖ Aggressively pursue NSA KMI initiative, address scalability issues
 - ❖ Deploy PKI-enabled subscriber security protocols: IPsec, SSL/TLS, S/MIME
 - ❖ Develop Type 1, high speed (multi-gigabit) IPsec devices
 - ❖ Constrain SIPRNET & JWICS network connectivity security policies
 - ❖ Deploy network infrastructure security technology: DNSSEC & S-BGP (under development now)
 - ❖ Deploy diverse intrusion detection systems at WAN & enclave boundaries and in hosts
 - ❖ Move all public DoD web sites off NIPRNET
 - ❖ Direct DISA to transition subscriber interfaces to IP (consistent with availability of suitable Type 1 crypto)
 - ❖ Employ spatial redundancy and design diversity for critical servers
 - ❖ Time: incrementally deploy with FOC NLT 2006
 - ❖ Total = \$1.5B over 5 years (a 50% increase over POM'd PKI/PKE initiative) & leverage IA R&D investment

Figure 58. Recommendation IV—Architecture

Finally, the GIG executive director should work through the CIO Executive Panel and the MCEB to implement the GIG system architecture. Specific system architecture and implementation issues that need immediate attention are noted in Figure 58. These include:

- Continuing to aggressively deploy PKI, and addressing scalability issues
- Aggressively pursuing NSA KMI initiative, addressing scalability issues
- Deploying PKI-enabled subscriber security protocols: IPsec, SSL/TLS, S/MIME
- Developing Type 1, high speed (multi-gigabit) IPsec devices
- Constraining SIPRNET and JWICS network connectivity security policies
- Deploying network infrastructure security technology: DNSSEC and S-BGP (under development now)
- Deploying diverse intrusion detection systems at WAN and enclave boundaries and in hosts
- Moving all public DoD web sites of NIPRNET
- Directing DISA to transition subscriber interfaces to IP (consistent with availability of suitable Type 1 crypto)
- Employing spatial redundancy and design diversity for critical servers

To support GIG implementation and to accelerate the DoD PKI/PKE strategy, the panel recommends an increase in budget of 50% over what is presently planned. This increase should not only accelerate the strategy, but also fund the development of Type 1 high-speed IPsec devices. This funding increase should be complemented and supported by the IA S&T investments called for in the companion report of the IA Technology Panel of the Defensive Information Operations summer study.

Architecture Recommendation V

- Executive director's system engineering office should establish a GIG IA R&D testbed
 - ❖ Develop metrics for protect, detect, and react (consistent w/ JV2020)
 - ❖ Combine real networks with simulation to achieve sufficient scale
 - ❖ Relate testbed experiments to real world via selected exercises and experiments
 - ❖ Test, evaluate, and determine vulnerabilities, including wireless
 - ❖ Transfer results to GIG as P3I
 - ❖ Provide feedback to industrial base
 - ❖ Time:
 - Establish version 1 testbed by 7/1/01
 - Support test, evaluation, and analysis efforts and testbed upgrades through 2006
 - ❖ Cost = \$200M over five years

Figure 59. Recommendation V—Testbed

The panel recommends that the executive director's system engineering office establish a GIG IA research and development testbed. The testbed nodes should be located at ESC, CECOM, SPAWAR, AFRL, NSA, etc. The participants in the evaluation process will include research and development, evaluation, and operational communities (services and agencies). The testbed will provide a means for measurement of system performance in the face of red team attacks on blue team scenarios and related information traffic. The testbed will also serve as a primary means for DARPA Information Assurance technology insertion and evaluation. The metrics and measurements will evolve as results are analyzed and lessons learned are derived from the data. Lessons learned will be fed back to red and blue teams to refine and update strategies and will be used by developers to improve system defenses. Lessons learned will also be made available to the GIG architects and system engineers to improve IA for the deployed system.

Finally, the testbed should be used to engineer, evaluate, and update defense-in-depth (DiD) strategies and technologies. The testbed will provide the means to understand residual DiD (and GIG) vulnerabilities and thus facilitate cost/benefit analysis for GIG IA investments. As noted in the panel's findings, no rigorous means for evaluating DiD systems, architectures, or technologies exist today.

The testbed should be implemented no later than July 2001, and augmented to support GIG IA technology, architecture, and metric evaluation over a five-year period.

Architecture Recommendation VI

- Director DII COE office should develop IA infrastructure consistent with GIG system architecture
 - ❖ Select operational application and integrate PKI with services (e.g., Common Operating Picture-COP)
 - ❖ Establish COE generic IA services using NSA KMI
 - ❖ Provide generic services as COE infrastructure and DoD PKI as available
 - ❖ Develop and deploy PKE COP by 9/1/02
 - ❖ Cost = \$10M over two years

Figure 60. Recommendation VI—IA Infrastructure

The panel recommends that the DoD begin the process of incorporating IA, and specifically PKI/PKE into the DII COE. In discussing alternatives with representatives from DISA, it was noted that the Common Operating Picture (COP) application is critical to CINC and services Joint-Task-Force-mission success. For a modest investment focused on PKE of this application, an acceleration of PKI into the COE, as generic, run-time utilities, can be accomplished. In addition to gaining important experience with PKE in battlefield applications, PKI could be integrated into the COE setting software standards and infrastructure for use in other service and CINC C4ISR systems.

Although IA infrastructure is planned to be incorporated into the COE "sometime in the future," the panel feels that accelerating this process is critical to ensure consistent PKE with tactical C4ISR systems. Experience gained sooner rather than later is key to effectively deploying an IA-enabled COE for the GIG.

APPENDIX A. TERMS OF REFERENCE



ACQUISITION AND
TECHNOLOGY

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

JAN 04 2000

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

**SUBJECT: Terms of Reference -- Defense Science Board Task Force on
Information Warfare - Defense**

You are requested to form a Defense Science Board (DSB) Task Force to review and evaluate DoD's ability to provide information assurance to carry out Joint Vision 2010 in the face of information warfare attack.

Tasks to be accomplished:

Using the "1996 DSB report on Information Warfare - Defense" as the departure point, address the following:

- What is the status of action on the recommendations?
- Where there are shortfalls, what are the barriers to action and what should be done?
- What important aspects did the 1996 Task Force miss that should have been addressed?
- Assess the recommendations of other important reports that have addressed information assurance issues.

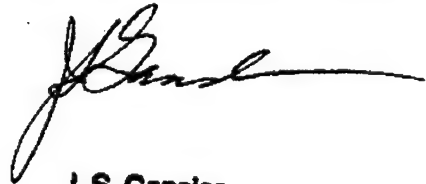
The Information Warfare - Defense Task Force will determine:

- Adequacy of the process toward the information assurance goals needed to carry out Joint Vision 2010.
- Adequacy of the Department's readiness to project and sustain power in the face of information warfare attacks.
- The appropriate role(s) and capability of DoD to provide information assurance in support of Homeland Defense and in support of Critical Infrastructure Protection.
- Recommendations for research and development which are uniquely in DoD's interest, and thus not likely to be accomplished by the private sector in the time required to meet DoD's Information Warfare - Defense objectives.
- Areas in which DoD should seek strong partnering relationships outside DoD, such as with the Critical Infrastructure Assurance Office (CIAO).
- The Task Force should provide an interim report by June 30, 2000.



The study will be co-sponsored by the Under Secretary of Defense (Acquisition, Technology and Logistics) and Assistant Secretary of Defense for C3I. Mr. Larry Wright will serve as the Task Force Chairman; Colonel Gregory Frick will serve as the Executive Secretary; and Major Tony Yang, USAF, will serve as the Defense Science Board Secretariat Representative.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5104.5, "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, United States Code, nor will it cause any member to be placed in the position of acting as a procurement official.

A handwritten signature in black ink, appearing to read 'J. S. Gansler', with a long horizontal flourish extending to the right.

J. S. Gansler

APPENDIX B. BIOS

DR. MICHAEL S. FRANKEL (Chair) is vice president and director of SRI International's Information, Telecommunications, and Automation Division. Dr. Frankel's expertise is in survivable command, control, and communication system design and implementation, radio frequency systems design and analysis, remote sensing, and data acquisition, reduction and analysis. Dr. Frankel is a Fellow of the IEEE and a member of the Cosmos Club, AFCEA, ADPA, Sigma XI and Tau Beta Pi. He received his B.S., M.S., and Ph.D. degrees in electrical engineering from Stanford University, California in 1968, 1970 and 1973, respectively. He was a member of the Army Science Board from 1992 through 1998, and served as its chair from 1996-98. When he left the Army Science Board, the U.S. Army awarded Dr. Michael Frankel the Distinguished Civilian Service Award. This award is the highest commendation that can be given to a civilian providing volunteer services to the Army and can only be bestowed by the Secretary of the Army. Dr. Frankel is presently a member of the Defense Science Board. He is the author or co-author of seventy SRI technical reports, over twenty publications in technical journals, and two textbook manuscripts. Dr. Frankel holds patent disclosures on passive satellite systems, a passive frequency-steerable microwave repeater system, an emitter location system, as well as one on the TeleEducation concept and a passive, high gain, frequency-steerable satellite repeater.

DR. STEPHEN THOMAS KENT is Chief Scientist- Information Security, BBN Technologies, Director- Security Practice Center, GTE Internetworking, and Chief Technical Officer, CyberTrust Solutions. Dr. Kent holds the following degrees: Ph.D, Computer Science, Massachusetts Institute of Technology, September, 1980; E.E., Electrical Engineering and Computer Science, Massachusetts Institute of Technology, February, 1978; S.M., Electrical Engineering and Computer Science, Massachusetts Institute of Technology, May, 1976; B.S., Mathematics, summa cum laude, Loyola University of New Orleans, 1973.

In his role as Chief Scientist, Dr. Kent oversees information security activities within BBN Technology, and works with government and commercial clients, consulting on system security architecture issues. In this capacity he has acted as system architect in the design and development of several network security systems for the Department of Defense and served as principal investigator on a number of network security R&D projects for almost 20 years. In his capacity as Director of the SPC, Dr. Kent monitors all security-related aspects of the service offerings of GTE Internetworking Services. He reports to the President of GTE Internetworking and coordinates with engineering, operations, and marketing to ensure the security quality of offerings. As CTO for CyberTrust Solutions, Dr. Kent provides strategic direction for this certification authority business, reporting to the President of CyberTrust.

During the last two decades, Dr. Kent's R&D activities have included the design and development of user authentication and access control systems, network layer encryption and access control systems, secure transport layer protocols secure e-mail technology, multi-level secure (X.500) directory systems, public-key certification authority systems, and key recovery systems. His most recent work focuses on public-key certification infrastructures for government and commercial applications, security for Internet routing, and high assurance cryptographic modules.

Dr. Kent served as a member of the Internet Architecture Board (1983-1994), and chaired the Privacy and Security Research Group of the Internet Research Task Force (1985-1998), both now under the auspices of the Internet Society. He chaired the Privacy Enhanced Mail (PEM) working group of the Internet Engineering Task Force (IETF) from 1990-1995 and co-chairs the Public Key Infrastructure Working Group (1995-). He was a charter member of the Board of the International Association of Cryptologic Research (1982-89) and served on the editorial board for the Journal of Telecommunication Networks (1982-1984). He currently serves on the editorial board of the Journal of Computer Security (1995) and on the board of the Security Research Alliance, a consortium of leading information security companies.

Dr. Kent served on the Information Systems Trustworthiness Committee (1996-98) of the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC). He was major contributor to the committee report, "Trust in Cyberspace." Previous CSTB/NRC service includes the committee on Rights and Responsibilities of Participants in Networked Communities (1993-94), the Technical Assessment Panel for the NIST Computer Systems Laboratory (1990-1992), and the Secure Systems Study Committee, which produced the "Computers at Risk: Safe Computing in the Information Age" report (1988-1990). Dr. Kent has often been called upon as a reviewer of CSTB committee reports.

The Secretary of Commerce appointed Dr. Kent as chair of the Federal Advisory Committee to Develop a FIPS for Federal Key Management Infrastructure (1996-98). The output of that committee forms the underpinning for a FIPS on Key Recovery. He previously served on the Presidential SKIPJACK Review Panel (1993-1994).

Dr. Kent has been an active participant in a number of professional conferences, as a speaker, session chair, program committee member, etc. He chaired the steering committee for the Symposium on Network and Distributed System Security (1990-1998) and was General Chair of the IEEE Symposium on Security and Privacy (1996-97). He has appeared as an invited speaker at security conferences throughout the United States, Europe and Asia.

Since 1977, Dr. Kent has lectured in the United States, Europe, Australia, and Asia on the topic of security in computer communication networks on behalf of various organizations, including the National Cryptologic School, George Washington University, M.I.T., University of Southern California, UCLA, various government agencies, and several private firms.

DR. PATRICK LINCOLN is the Director of the Computer Science Laboratory of SRI International, a leading center for research on the fundamental issues of computer security, networks, and automated formal methods. Under his direction, the lab is expanding its presence in these areas and is extending its research agenda into new areas. Dr. Lincoln joined SRI in 1992 after completing Ph.D. work at Stanford University in Computer Science. He holds a B.Sc. from MIT and has previously held positions at MCC and Los Alamos National Laboratory. Dr. Lincoln is an active researcher in the fields of networks, security, language design, and mobile code. He has published widely and made significant contributions to the formal analysis of systems, languages, and protocols in computer security, safety, and fault tolerance, and to their integration into survivable systems. He serves on the Digital Island (Nasdaq:ISLD) Strategic Advisory Board. <http://www.csl.sri.com/~lincoln>

ALAN J. MCLAUGHLIN received BS and MS degrees in Electrical Engineering from Northeastern University in 1957 and 1959, respectively. During 1959-60 he served as a Lieutenant in the U.S. Army Signal Corps Laboratories at Fort Monmouth, NJ. He was awarded the Army Commendation Medal for meritorious service. From 1961-71 he was a Lecturer at the Northeastern University Graduate School of Engineering.

From 1960 to 1962 he was a project engineer with Contronics, Inc., engaged in the design and development of automatic test equipment. He joined the engineering staff of Deco Electronics, Inc. in 1962, where he designed digital communications equipment. In 1965 he became a systems engineer with General Instrument Co., where he was involved with the design of sonar systems and associated signal processing equipment.

In 1967 Mr. McLaughlin joined the staff of MIT Lincoln Laboratory. Initially he was engaged in the design of special-purpose processors for anti-jam communications systems and later with the design of high-speed signal processors. He established a laboratory for the investigation of GaAs laser diode parameters and participated in the design of an optical communications system. In 1972 he joined the Education Technology Group where he was responsible for the design of Computer-Aided Training systems. In 1974 he was appointed Leader of the Education and Computer Technology Group.

In 1975 he was appointed Associate Head of the Computer Technology Division and a member of the Lincoln Laboratory Steering Committee. In 1978 he was appointed Head of the Computer Technology Division with management responsibility for laboratory programs in speech, radar and image signal processing, computer networks, digital processor technology, digital integrated circuits and machine intelligence technology. In 1992 he was appointed Assistant Director of Lincoln Laboratory. He is currently responsible for Advanced Electronic Technology, Air Traffic Control and Surface Surveillance programs at the Laboratory.

In 1978-79 Mr. McLaughlin served on an Air Force steering committee for advanced computer technology planning. In 1980-81 he served on a National Academy of Science study committee on modernization of Air Force computerized administrative support systems. In 1984-85 he was a member of a senior advisory committee to the Director of ARPA in the area of information processing. Since 1986 he has been a member of the ARPA Information Science and Technology Study Group. In 1988-89 he served as co-chairman and in 1990-91 chairman, of the ARPA Study Group. In 1991-92 he served on a National Academy of Science study committee on Modernization of the Worldwide Military Command and Control Information System. In 1993 he served on the Air Force Scientific Advisory Board Study on Information Architectures. In 1994-95 he served on a National Research Council Committee on Future Technologies for Army Multimedia Communications. He has served on a variety of Defense Science Board task forces: 1994-95 Acquiring Software Commercially, 1996 Defensive Information Warfare, 1996-97 Aviation Safety, 1997-98 Military Excess and Surplus Material, 1999 Investment Strategy for DARPA. Mr. McLaughlin is a member of Eta Kappa Nu and a Senior Member of the IEEE.

PETER STEENSMA is Chief Scientist and Senior Technical Director, ITT Aerospace Communications Division. He received his B.S. degree at Calvin College in Physics, Mathematics, and German Literature; his M.S. was received from the Polytechnic University of Brooklyn; and he was a Research Associate at Princeton University.

Mr. Steensma has 30 years of communications systems design and development experience, including mobile tactical networks, tactical switching, radio and optical fiber transmission, secure command and control networks, and satellite and terrestrial radio navigation.

Recent highlights include:

- Initiated and provided technical leadership to several programs aimed at establishing the next generation of mobile tactical communications systems, including Hand-held Multimedia Terminal and Small Unit Operations DARPA programs
- Formed international consortium of 12 nations and established a multinational joint venture company, TACONE, to set next generation NATO post 2000 communications standards
- Led conceptualization and development ITT communications products in the Tactical Internet, including SINCGARS radios (SIP and ASIP), Near Term digital Radio (NTDR), and the Internet Controller. These supported the US Army TF XXI exercises and subsequent digitization efforts
- Technically led a winning US/UK team for UK Project Bowman, a total Forward Area Battlefield Communications System for the United Kingdom Ministry of Defense. Led the development and demonstration of a Product Demonstrator, the first mobile tactical internet system. Continuing responsibility and support for developing production solution

Past positions include, Director of Systems Engineering, Director of Internal Research and Development, Manager of C2 Systems Engineering, Senior Scientist Transmission Systems.

JOHN WOODWARD is the Technical Director of the Intelligence and Special Programs Division, which executes MITRE's \$35M Air Force intelligence program. Mr. Woodward also serves as corporate Director of Information Warfare, where he is responsible for ensuring that MITRE's varied information warfare activities are coordinated, responsive to broad government objectives, and of high quality.

Mr. Woodward has more than 25 years of experience in software engineering with MITRE, and has specialized in information system security for the past 22 years. Prior to his present position, he was the Associate Technical Director of the Information Systems Security Division, where he shared management responsibility for MITRE's technical center providing information security and defensive information warfare expertise throughout MITRE, and to MITRE's Department of Defense, intelligence, and Federal Aviation Administration customers.

In earlier positions at MITRE, he managed the prototype development of the Joint Worldwide Intelligence Communications System, and was responsible for MITRE's intelligence information system support to the Defense Intelligence Agency, North American Air Defense/U.S. Space

Command/Air Force Space Command, and the Strategic Air Command. He also led MITRE's Artificial Intelligence Technical Center. He was responsible for inventing, prototyping, and specifying compartmented mode workstations, which are now available commercially from multiple vendors. He also created and was the original chairman of MITRE's Information Policy Committee.

Mr. Woodward received masters and bachelor's degrees in applied mathematics/computer science in 1974 from Brown University.

APPENDIX C. AGENDAS

DSB Agenda 22-23 Feb 2000

**To be held at the offices of
Strategic Analysis, Inc.
3601 Wilson Blvd., Suite 600
Arlington, VA 22201**

Tuesday, February 22, 2000

0845 - 0900	Administrative Remarks	Mr. Wright and Col Frick
0900 - 1000	Eligible Receiver/Solar Sunrise	Lt Col Perry Luzwick, OSD
1000 - 1100	* Classified (Network Intrusion)	CDR Bob Gourley, JTF-CND
1100 - 1200	DoD Insider Threat IPT results	Mr. Tom Bozek, OSD
1200 - 1300	Lunch/Free Discussion	
1300 - 1400	Global Information Grid Architecture	Mr. John Osterholz/Mr. Terry Hagle, OSD
1400 - 1500	DoD Web Security Initiatives	Ms. Linda Brown, OSD
1500 - 1630	* Classified DIA Threat/I&W	John Yurechko
1630	Summary/Wrap-up/Time for Panels as needed	

Wednesday February 23

0845 - 0900	Administrative Remarks: Mr. Wright/Col Frick	
0900 - 1100	* Classified NSA Overview to include threat/red teaming/strategy	Mr. Larry Castro/CAPT Ed Kinerva
1100 - 1200	Navy IA overview/capabilities	CAPT James Newman
1200 - 1300	Lunch/Discussions	
1300 - 1400	AF IA overview/capabilities	Lt Col Dave Warner/Lt Col Susan Pardo
1400 - 1500	Army IA overview/capabilities	Mr. Phil Loranger/LTC Krist
1500 - 1600	DISA IA overview/vision (pending) or time for panel breakouts	

Note: morning and afternoon breaks will be taken as needed. Original plans for this plenary session included a brief from DTRA (ruling was that it can be given at the future but only at SCI level) and Kosovo Lessons Learned (still trying for this, but releasability issue with Joint Staff at this time).

DSB Agenda 27-28 March 2000

To be held at the offices of
Strategic Analysis, Inc.
3601 Wilson Blvd., Suite 600
Arlington, VA 22201

Monday, March 27, 2000

0845 – 0900	Administrative Remarks	Mr. Wright and Col Frick
0900 - 1000	Army IA Initiatives	LTC Lundgren
1000 - 1200	Panel Chairs Outbrief Progress/Issues to Date	
1200 – 1300	Lunch/Free Discussion	
1300 – 1430	Joint Staff Perspectives	BG Quagliotti, Joint Staff/J6
1430 – 1530	CIAO/National Plan	Mr. John Tritak
1530 - 1630	Industry IA Perspectives	Mr. Chris Christiansen, IDC
1630	Wrap up	

Tuesday, March 28, 2000

0800 – 0830	Opening Remarks	Dr. Mike Frankel <i>Panel Chairman</i>
0830 – 0930	Defense in Depth II	Col Pat Phillips <i>J6K</i>
0930 – 1030	Information Assurance Technical Framework (IATF)	Dave Luddy <i>NSA</i>
1030 – 1100	Break	
1100 – 1200	Network Management System (NMS)/ Base Information Protect Air Force	COL Roger Robichaux <i>Air Force</i>
1200 – 1:00	Lunch/Discussions	
1:00 – 2:00	GIG IA Architecture Overlay	Terry Mayfield <i>IDA</i>
2:00 – 3:00	I3A	Mr. Doug Troester <i>MITRE</i> LTC Roy Lundgren
3:00 – 3:15	Break	
3:15 – 4:45	Discussion	
4:45 – 5:00	Wrap-up	

AGENDA
DSB Task Force on Defensive Information Operations
April 19-20, 2000
Booz-Allen & Hamilton
Hamilton Building Room 2014

April 19, 2000		
0730	Registration	
0800	OSD Human Resources IPT Studies	CAPT Katherine Burton
0900	Joint Vision 2010/2020	Col Andrew Twomey
1000	DoD PKI Program	Mr. Mike Green
1100	DISA Future Concepts	Mr. Richard Hale
1200	Lunch/Overflow of morning briefs	
1300	Logistics IA study: Theater Distribution	Ms. Virginia Wiggins
1400	TRANSCOM IA Initiatives/GTN	Jacques Sabrie
1500	InfoSec Research Council (IRC)	Dr. John McLean Dr. Carl Landwehr
1600	DARPA Initiatives	Dr. William Mularie
April 20, 2000	Sub-Panels meet	

DSB IAA PANEL
Agenda 20 April 2000

Thursday, April 20, 2000

0800 – 0830	Opening Remarks	Dr. Mike Frankel <i>Panel Chairman</i>
0830 – 0930	Navy/Marine Corps Intranet	Mr. Scott Henderson <i>SPAWAR</i>
0930 – 1030	DII Security Architecture	Mr. Richard Hale <i>DISA</i>
1030 – 1100	Break	
1100 – 1130	ISO Security Reference Model	Dr. Stephen Kent <i>BBN Technologies</i>
11:30-12:00	Lincoln Lab Security Metrics	Mr. Alan McLaughlin <i>MIT/LL</i>
12:00 – 12:30	Lunch/Discussions	
12:30 – 1:15	Gold Security Architecture Reference Model	Mr. Terry Mayfield <i>IDA</i>
1:15 – 2:00	IA Operation Readiness Metrics	LtCol Lisa Lemza J-6
2:00 – 2:15	Break	
2:15 – 5:00	Discussion and Wrap-up	

Agenda
Defense Science Board Spring Quarterly Meeting
May 24-25, 2000
Thursday, May 25, 2000 (3E869)

0800	Defensive Information Operations Study	Mr. Larry Wright
0830	Network Security & Architecture	Dr. Michael Frankel
0900	Defensive Information Operations Legalities	Mr. Stewart A. Baker
0930	Defensive Information Operations Organization	MGEN John P. Casciano, USAF (Ret.)
1000	General Henry Shelton, USA, CJCS	
1030	Break	
1045	Defensive Information Operations Policy	Mr. Richard Wilhelm
1115	Defensive Information Operations Technology	Mr. Richard M. Mendelowitz
1200	Lunch in Blue Room (3D854) hosted by Hon. Jacques S. Gansler, Under Secretary of Defense (Acquisition, Technology & Logistics)	
1315	Annual Group Photo (River Entrance)	
1330	Intelligence Needs for Civil Support	Dr. Ruth David Mr. Peter Marino
1430	Hon. Jacques S. Gansler	
1530	Closing Comments	DSB Chairman
1545	Adjourn	

DRAFT AGENDA

MAY 26, 2000

**DSB TASK FORCE ON DIO
STRATEGIC ANALYSIS, INC.
3601 WILSON BLVD. SUITE 600
ARLINGTON, VA 22201**

Time	Topic	Briefer
0800	Pervious DARPA IA perspective	Sami Saydjari
0900	DARPA IA (follow-on)	Mike Skroch
1000	USSPACE	Col Larry Klooster
1100	CISCO perspectives	J. Romain
1200	Lunch	
1300	Biometrics	Jeff Dunn, NSA
1400	NSA Senior IA perspectives	John Nagengast
1700	Adjourn	

**DRAFT AGENDA
DSB TASK FORCE ON DIOAT
SAIC SCIF
4001 N. Fairfax Drive, Suite 500
Arlington, VA
Tuesday, June 13, 2000**

TIME	TOPIC	BRIEFER
0800-0930	Performance Needs/Developing technology	Lee Hammarstrom & Pat Dowd
0930-1030	Chessmaster and recent events	Mike Shore
1030-1200	History of IW	ADM Bill Studeman, USN (Ret)
1200-1:00	Lunch	
1:00-2:00	CIA Strategic Warning/ Threat	Dr. Tom Donahue
2:00 – 3:00	Discussion	
3:00 – 4:30	IA Metrics	Mr. Terry Bartlett/DIAP
4:30 – 5:00	Wrap-up	

**DSB IAA PANEL
Agenda
June 14, 2000
To be held at the offices of
Strategic Analysis, Inc.
3601 Wilson Blvd., Suite 600
Wednesday, June 14, 2000**

7:30 – 8:00	Coffee – Sign-in	
8:00 – 9:00	TA Security Standards	Mr. James Barnette DISA
9:00 – 9:30	Results of a DARPA sponsored study on "Information Assurance for Mobile Operations" An approach and some preliminary results on: "Intrusion Detection for the Lower Tactical Internet"	Mr. Al McLaughlin/MIT/LL
9:30 – 9:45	Break	
9:45 – 12:00	Architecture Development and Recommendations	
12:00 – 12:30	Working Lunch	
12:30 – 3:30	Architecture Development and Recommendations	

DSB IAA PANEL
Agenda
July 12-14, 2000
To be held at the offices of
Strategic Analysis, Inc.
3601 Wilson Blvd., Suite 600

Wednesday, July 12, 2000

TIME	TOPIC	BRIEFER
8:00 – 8:30	Coffee - Sign-in	
8:30 – 10:30	IAA Introduction	Dr. Mike Frankel
10:30 – 10:45	Break	
10:45 – 11:45	IA Wireless Issues	Mr. Pete Steensma
11:45 – 12:30	Lunch	
12:30 – 1:30	Reference Model	Dr. Stephen Kent Dr. Patrick Lincoln Mr. John Woodward
1:30 – 2:30	IA Metrics/Standards	Mr. Al McLaughlin
2:30 – 3:30	Technical Architecture	Dr. Stephen Kent Dr. Patrick Lincoln Mr. John Woodward
3:30 – 4:30	System Architecture	Dr. Stephen Kent Dr. Patrick Lincoln Mr. John Woodward

Thursday, July 13, 2000

8:00 – 8:30	Coffee – Sign-in	
8:30 – 10:00	COE	Mr. Ken Wheeler DISA
10:00 – 11:30	JWICS	Mr. Jim Watson DIA
11:30 – 12:30	General Issues Discussion	All
12:30 – 1:00	Lunch	
1:00 – 5:00	Integrate Briefings	All

Friday, July 14, 2000

8:00 – 8:30	Coffee – Sign-in	
8:30 – 9:00	Front End of Outbrief	Larry Wright
9:00 – 9:15	Findings & recommendations – Legal Panel	Stewart Baker
9:15 – 9:30	Findings & recommendations – Policy Panel	Rich Wilhelm
9:30 – 9:45	Findings & recommendations – Organization Panel	John Grimes
9:45 – 10:00	Findings & recommendations – Technology Panel	Rich Mendelowitz
10:00 – 10:15	Findings & recommendations – IAA Panel	Mike Frankel
10:15 – 15:00	Task Force Discussion on outbrief and other issues	All

APPENDIX D. ACRONYMS

ABIS	Advanced Battlefield Information System
AFRL	Air Force Research Laboratory
AH	Authentication Header
ARL	Army Research Laboratory
ASD/C3I	Assistant Secretary of Defense for Command, Control and Communications
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
BSC	Base Switching Center
BTS	Base Transmission System
C2	Command and Control
C3I	Command, control, communications, and intelligence
C4ISR	Command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAC	Common Access Card
CAP	Common Air Picture
CC	Common Criteria
CCA	Clinger-Cohen Act
CCITT	Consultive Committee on International Telegraph and Telephone
CDPD	Cellular Digital Packet Data
CEC	Cooperative Engagement Capabilities
CECOM	U.S. Army Communications Electronics Command
CERT	Computer Emergency Response Team
CGP	Common Ground Picture
CINC	Commander in Chief
CIO	Chief Information Officer
COE	Common Operating Environment
COI	Community of interest Connection-oriented interconnection
COMSEC	Communication Security
CONUS	Continental United States

COP	Common Operational Picture
CORBA	Common Object Request Broker Architecture
COTS	Commercial off the shelf
CVE	Common vulnerabilities and exposures
DARPA	Defense Advanced Research Projects Agency
DBS	Direct Broadcast Satellite
DCE	Distributed computing environment
DDR&E	Director Defense Research and Engineering
DEERS/RAPIDS	Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System
DFAR	Department of Defense Federal Acquisition Regulation Supplement (DoD)
DEPSECDEF	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DIAP	Defense-wide Information Awareness Program
DiD	Defense in Depth
DII	Defense Information Infrastructure
DISC4	Director of Information Systems, Command, Control, Communications, and Computers
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DIRNSA	Director National Security Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security
DoD	Department of Defense
DoS	Denial of Service
DOTMLPF	Doctrine, Organization; Training and Education, Materiel; Leadership; Personnel; and Facilities
DSB	Defense Science Board
DSL	Digital Subscriber Line
EJB	

ESC	Electronic Systems Center (U.S. Air Force)
FGAC	Fine grained access control
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GIG	Global Information Grid
GloMo	Global Mobile
GSM	Ground station module
HLR	Home Location Register
HQ	Headquarters
HQMC	HQ Marine Corps
IA	Information Assurance
IAA	Information Assurance Architecture
IATF	Information Assurance Technical Framework
IC	Intelligence Community
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IASA	Information Assurance Systems Architecture
IATA	Information Assurance Technical Architecture
IATF	Information Assurance Technical Framework
ICMP	Internet Control Message Protocol (DoD, TCP/IP)
IER	Information Exchange Requirements
IETF	Internet Engineering Task Force
III	Integrated Information Infrastructure
IKE	Internet Key Exchange (previously ISAKMP)
IM	Information Management
IN	Intelligent Network
INFOCON	Information condition
InfoSec	Information Security
IO	Information operations
IOC	Initial Operational Capability
IP	Internet Protocol

IPsec	Internet Protocol security
IS	Information Superiority
ISDN	Integrated Service Digital Network
ISO	International Organization of Standardization
ISP	Internet Service Provider
ISR	Intelligence, Surveillance and Reconnaissance
ISX	Information Superiority Experiment
IT	Information Technology
ITEF	Internet Engineering Task Force
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union (CCITT)
IW-D	Information Warfare-Defense
JCS	Joint Chiefs of Staff
JFCOM	Joint Forces Command
JIER	Joint Information Exchange Requirements
JMRR	Joint Mission Readiness Report
JOA	Joint Operational Architecture
JROC	Joint Requirements Oversight Council
JSA	Joint System Architecture
JSMB	Joint Space Management Board
JSTARS	Joint Surveillance Target Attack Radar System
JTA	Joint Technical Architecture
JTF	Joint Task Force
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
JV 2020	Joint Vision 2020
JWICS	Joint Worldwide Intelligence Communications System
KMI	Key Management Infrastructure
LAN	Local Area Networks
LDAP	Lite Directory Access Protocol
LEO	Low Earth Orbiting

LMDS	Local Multipoint Distribution System
M&S	Modeling and Simulation
MCEB	Military Communications Electronics Board
MEO	Mid Earth Orbiting
MIL-STD	Military Standard
MMDS	Multichannel Multipoint Distribution System
MRC	Major Regional Conflict
MSC	Mobile Switching Center
MSP	Message Security Protocol
NEO	Near Earth Orbit
NIAP	National Information Assurance Partnership
NIPRNET	Non Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NRE	Non-Recurring Engineering
NRL	Naval Research Laboratory
NRO	National Reconnaissance Office
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
NSB	Naval Studies Board
O&M	Operation and Maintenance
OA	Operational Architecture
OASD/C3I	Office of the Assistant Secretary of Defense, Command, Control, Communications & Intelligence
OMFTS	Operational Maneuver from the Sea
OODA	Observe, Orient, Decide, Act
OPFAC	Operations Facility
OPGP	Open PGP (Pretty Good Privacy)
OPNAV N6	Navy Operations
OPNET	Operations Network
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense

OSI	Open Systems Interconnect
PA&E	Program Analysis and Evaluation
PCS	Personal Communications Systems
PDA	Personal Digital Assistants
PEM	Privacy Enhanced Mail
PEO	Program Executive Office
PFF	Packet filtering firewall
PGP	Pretty Good Privacy
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PKIX WG	Public Key Infrastructure Working Group
PM	Program Manager
POM	Program Objective Memorandum
POP	Point of presence
PPP	Point to Point Protocol
PSTN	Public Switched Telecommunications Network
QoS	Quality-of-service
R&D	Research and Development
RM	Reference Model
RSTA	Reconnaissance, Surveillance and Target Acquisition
RSVP	Resource Reservation Protocol
RTP	Real Time Protocol
S&T	Science and Technology
S-HTTP	Secure HyperText Transfer Protocol
SA	System Architecture
SDE	Secure Data Exchange
SET	Secure Electronic Transactions
S-BGP	Secure Boundary Gateway Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SCP	Service Control Point
SILS	Standard for Interoperable LAN Security

SINCGARS	Single Channel Ground and Airborne Radio System
SIPRNET	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPAWAR	Space and Naval Warfare Systems Command (formerly NAVELEX)
SPKI	Secure Public Key Infrastructure
SSH	Secure Shell
SSL	Secure Socket Layer
SSNMP	Secure Simple Network Management Protocol
SSP	Switching Signal Point
STP	Signaling Transfer Point
SUO	Small Unit Operations
SYN	Synchronization
TA	Technical Architecture
TAFIM	Technical Architecture Framework for Information Management
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
TLSP	Transport Layer Security Protocol
TOR	Terms of Reference
TRANSEC	Transmission Security
TTP	Tactics, techniques and procedures
UHF	Ultra High Frequency
UL	Underwriters Laboratories
USAF	U.S. Air Force
USCG	U.S. Coast Guard
USD/AT&L	Under Secretary of Defense for Acquisition, Technology and Logistics
USPACOM	U.S. Pacific Command

AOAR	Area of Assigned Responsibility
VCJCS	Vice-Chair Joint Chiefs of Staff
VoIP	Voice over Internet Protocol
VLR	Visitor Location Register
VPN	Virtual Private Network
WAN	Wide area network
WIN-T	Warfighter Information Network-Tactical
WWW	World Wide Web
XML	Extensible Markup Language

ANNEX B

Defense Science Board Task Force on Defensive Information Operations

Panel Report on Technology

REPORT OF FINDINGS, DISCUSSION/OBSERVATIONS AND RECOMMENDATIONS

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
INTRODUCTION.....	3
RESEARCH TOPICS	7
Early Capability Assessment	7
Prevention and Protection	8
Consequence Management	12
Attribution.....	13
CROSS-AREA RESEARCH	15
Modeling and Simulation.....	15
Theory of Vulnerabilities	15
Interdependencies	15
Broad-Based Fundamental Research	16
GIG Research Coordination.....	16
Costs.....	17
CONCLUSIONS AND RECOMMENDATIONS	19
APPENDIX A. Task Force members.....	A-1
APPENDIX B. Acronyms.....	B-1

EXECUTIVE SUMMARY

Within the Department of Defense, the next several years will be marked by steadily increasing reliance on automated information systems. In accord with Joint Vision 2020 (JV2020), the Department will be proactive in supporting and shaping this evolution.

In recognition of this reliance on information systems and in reaction to attacks on DoD computer systems, the Department has begun a wide range of activities that focus on prevention of problems through protection of computer networks. The rapid advances in information and communications technology mean that as the years pass, entirely new infrastructures, embodying new technologies, will emerge – and each will be accompanied by its own set of new vulnerabilities. As a result, protection of networks will necessarily require continuous improvement. These protections will require vigorous and focused research. It is the view of this Technology Panel that an increase in research beyond current levels is required to minimize the vulnerability gap that will always exist between network vulnerabilities and network protection. It should be noted that DoD requirements for protection are likely to go well beyond what is required by the private sector.

As computer networks and weapon systems lose their individual identity and merge into one, protection will be necessary, but not sufficient to assure that networked information will be available when required. As this Defense Science Board has noted, despite the best network protection, attacks will occur and some will succeed. When a computer network has been attacked, the commander must be able to know:

- When will the system be restored?
- How much of the system will be restored?
- How much of the original system will operate?
- What are the consequences of limited network availability?
- Will the information on the network be reliable?
- How will the commander know for sure that the information is reliable?
- What options will be available to the commander?

Today, the answer to these questions would be, “We do not know.” This is clearly a bad answer in peacetime and a totally unacceptable answer during a military operation.

The Department has reached a milestone with its awareness of computer network vulnerabilities, and with funded programs to address protection and defense of networks. Unfortunately, while restoration of network service, data integrity, and confidence in the data on the network are as important to success of JV2020 as network protection, these activities remain largely ignored and are essentially unfunded. Successful development and implementation of these “consequence management” functions are the next major milestone for DoD Information Assurance (IA).

The Department must also aggressively address its information assurance (IA) research and development (R&D) personnel requirements now, in order to avoid more serious problems in the next few years as more personnel leave the Department and fewer high-caliber R&D managers remain. Although this topic is addressed more extensively by another Panel report, we believe it is so fundamental that we endorse and highlight the finding. Education and training issues must be among the very first steps that the Department should take in this area. As urgent as the other IA technology issues are that we discuss below, this issue is the highest priority in the technology area. Without enough qualified and well-trained technical people, virtually all of the issues that the Department faces in IA will be even more difficult to resolve.

Protection of DoD networks is fundamental to the success of future operations, and this protection depends upon a very focused R&D program. However, this Panel finds that IA R&D activities are distributed among the Defense Advanced Research Projects Agency (DARPA), the services, and defense agencies. Some long-term research is ignored, and some short-term research is redundant. Accordingly, this Panel proposes a new and very focused management of IA R&D. Establishing an information assurance R&D office in the Office of the Secretary of Defense (OSD) that reports to the Global Information Grid (GIG) architect is the first step in bringing focus to IA R&D management. This R&D office will assure that DoD research for IA be coordinated, be subject to multi-year planning, take into account private-sector research, and be adequately resourced to minimize DoD network vulnerabilities on a rapid but achievable timetable. Given today's commercial product cycles, it is unlikely that any new DoD-sponsored research will produce protection results that can be transferred within three years into critical networks. DoD research must therefore be a long-term, continuous investment activity that should not be expected to play a significant role in the near term.

Moving resources from minimally funded protection activities to network restoration activities will not result in an acceptable solution for either problem. Establishing a new milestone of consequence management calls for additional funding. Since the commercial world has largely ignored this issue, solutions will have to start with a vigorous DoD R&D program. This Panel believes that the minimum R&D investment that should be added to current efforts to improve the overall security of the GIG is \$350 million over five years-- about twice the level of funding today.

INTRODUCTION

The 1996 Defense Science Board (DSB) Summer Study brought attention to the increasing reliance of DoD on networked computer systems. The DSB report noted the vulnerability of these computer systems, and the fragility of the information residing on and passing across these networks. It made strong recommendations that the Department increase emphasis on the protection of these systems and the information they held. The report also recommended that computer network defense (CND) become integral to the development and deployment of DoD networks.

During the four years since that report, the Department has made considerable progress on these recommendations. Awareness of computer network vulnerabilities is much higher, and various system components have been deployed specifically for network security. Research programs, principally at DARPA and the National Security Agency (NSA), have emphasized those defensive technologies that DoD requires but commercial systems are unlikely to include.

However, during that same period of time:

- DoD has greatly increased its reliance on information contained in, processed by, and distributed over networked computer systems.
- Information superiority has become essential to achieving JV2020. This vision requires highly secure networked systems.
- Intrusions into DoD networked computer systems have become more sophisticated and more frequent. (The frequency of these intrusions is similar to what is being experienced in the non-DoD environment.)
- Development and deployment of new network technology has greatly outpaced information assurance technology, increasing the vulnerability of DoD systems.

As a result, despite the considerable progress that is apparent within DoD, a computer network vulnerability gap has continued to increase. Systems complexity is growing faster than solutions. And while new network capabilities will most certainly always outpace defensive technologies, considerable DoD R&D must be devoted to computer network defense to manage and reduce the vulnerability of this critical capability.

Potential adversaries have recognized both the increasing reliance of DoD on networked computer systems and the opportunity they now have to diminish the effectiveness of DoD operations through active network attacks. For example, representatives of both China and Russia have expressed the belief that they can neutralize U.S. capabilities through information operations. The "Unrestricted War" concept from China and the Russian nationalist Vladimir's comment that "we can bring the entire West to its knees with our computer specialists" are examples of that thinking.

In order to assure the availability and integrity of critical DoD computer networks, the Department must develop a long-term strategy that posits a desired end-state for information assurance that is consistent with JV2020 and provides a roadmap for achieving that end-state. While many areas need to be included in an overall roadmap, the information assurance R&D

roadmap is fundamental. The key for DoD to be prepared on the scale required is an information assurance R&D program supporting the protection needs of the global information grid.

The information volume that JV2020 will need to handle and protect will be vast. It is already possible to project data rates that will require protection in the range of multiple terabits per second. These rates are comparable to moving the current Library of Congress electronically every minute. The DoD and intelligence databases in 2020 almost certainly will be many hundreds of times those of the current Library of Congress. While secure remote access to data will reduce somewhat the requirement for data rates and bandwidth that increase in proportion to the size of databases, it is still obvious that protecting information in the volumes required for successful execution of JV2020 will be a daunting task.

It has recently been understood that no matter how sophisticated defense of computer networks becomes, they will remain vulnerable to a determined adversary, disgruntled employee, or simply natural events. Experience shows that as our defensive capabilities increase, so will the adversary's offensive ones. U.S. adversaries over the next 20 years will be developing a range of attack capabilities that will likely cover every possible node and path of DoD networks.

There will certainly be attacks against DoD networks. Many will be ineffective, but more importantly *some attacks will succeed*. The results of a successful attack will range from an irritation or embarrassment all the way to serious disruption of critical DoD networks or information. The severity will depend on the attacker's skill level and resources, and the defenses DoD has in place. These attacks could result in serious damage to a critical DoD network, but could also compromise a warfighter's confidence in the information system he or she has to rely on – no matter what the attack actually accomplished.

Unfortunately, today DoD has no methodology for dealing with the consequences of a successful attack and restoring integrity in its systems. And so, with the ever-increasing reliance of DoD on computer networks as an integral component of war fighting, **this Defense Science Board finds that it is now necessary to develop technologies to help recover and restore its networks and the data they contain**. One of the key tasks in this area will be to restore the integrity of networked computer systems that have been attacked, or are thought to have been attacked, and restore confidence that they remain ready for their intended purpose. Warfighters must have confidence in their information and the technology that provides it. The technologies that will deliver effective defense in depth of DoD, be able to recover and reconstitute those networks after an attack, and restore their integrity, need considerable emphasis.

It should be noted that any list of research areas compiled today would certainly not be a complete list for tomorrow. Part of the information assurance R&D management challenge in the rapidly evolving world of information technology, is the frequent examination of those research areas most needed to provide defense of and integrity restoration to the latest computer network developments and deployments. Against the tide of technological advances and determined adversaries, considerable R&D will be required just to maintain the level of security we have today. Much of the R&D required by the DoD will not come from the private sector. To achieve and maintain the higher levels of protection required by JV2020, it will be necessary for DoD R&D investment to keep pace.

The DoD must provide the support for an aggressive R&D program that has the breadth and depth to deal with the entire spectrum of information assurance issues. These issues range from near-term needs to thwart the latest threats that surface, to long-term basic research. The latter

must be coupled with an examination of the R&D strategies necessary to satisfy the full range of JV2020 requirements. Further, the R&D program must result in products that are unique to DoD requirements and which complement and enhance commercial systems. Many of these research programs will necessarily be long term—not suited to short-term evaluations.

The specific amount of R&D funding required is likely to be a matter of debate, but the general level needed is at least a factor of two over the DoD information assurance R&D spending of today. There are many areas that are today minimally funded, which this report highlights. There are certainly many more areas that time did not allow us to pursue, or that have simply not yet been articulated.

RESEARCH TOPICS

The pace of technology growth guarantees that any list of needed research topics will be incomplete shortly after it is written. Part of the information assurance R&D management challenge in the rapidly evolving world of information technology is the frequent examination and re-evaluation of those research areas most needed to provide defense of and integrity restoration to the latest computer network developments and deployments.

Keeping in mind the need for frequent re-evaluation of R&D programs in light of commercial developments, research successes, and new deployments, there are four general topic areas that prove useful in categorizing R&D for computer network defense. This report provides findings on areas of necessary research in each category of a network attack timeline, namely:

1. Early Capability Assessment
2. Prevention and Protection
3. Consequence Management
4. Attribution

What follows is a general description of each of these topics together with some representative technologies that this Panel feels currently need increased attention.

EARLY CAPABILITY ASSESSMENT

Computer network defense, like any defense, is most effective if the intentions and capabilities of an identified adversary are understood, and when it is known that offensive operations have, in fact, begun. The technology for this entire area of intelligence, indications and warning, intention, and identity-determination is complicated by legal and policy issues, which are discussed elsewhere in this report. Examples exist today of attacks which have gone unnoticed, of intrusions with unknown purpose, and of network disruptions that have remained un-diagnosed. This is a technology area that must mature as JV2020 develops. Some necessary research topics include the following.

Cyber Intelligence Tools

One of the weakest aspects of U.S. defensive information operations is our extremely limited ability to detect, assess, and understand both hostile information operations (IO) capabilities and precursor indications and warning of attack. A program is required to develop tools to attenuate these shortcomings. Advanced active agents using secure mobile code would be developed that could gather information without taking any hostile actions. "Picket" or "sentinel" agents could provide early warning of hostile action or intent. This program will ideally result in an array of tools that will provide a much greater understanding of hostile IO capabilities against the United States and its allies and better warning of incipient attacks.

Attack Pattern Discovery

No methods exist for automated or assisted discovery of existing or novel attack patterns or signatures, particularly for those attacks that are distributed across many computers or networks.

PREVENTION AND PROTECTION

Much of the progress within DoD since the 1996 DSB report has been in the area of protection of DoD networks and prevention of unauthorized access. These are very important and sensible places to begin the defense process. However, as DoD becomes more and more dependent on networks, and as the complexity of these networks increases, the opportunities for disruption will also increase. R&D is required that is specifically designed to prevent problems caused by both insiders and outsiders, to prevent unknown attacks, and to guard against commercial systems with unknown flaws. The science of network security is currently immature, but with proper R&D infusion, the foundation for the protection required by JV2020 can be put in place.

Representative areas of research to enhance protection of DoD networks and prevention of unauthorized access would include those that follow.

Scalable Global Access Control

Current DoD network architecture calls for a secure network with authorized access via tokens – a public key infrastructure (PKI). The scope of this security apparatus is enormous. It will involve distribution of secure capability to multiple locations in many countries. It will require limited access for foreign coalition partners. It will necessitate the distribution of millions of tokens – some number of which must be issued and revoked on a daily basis. It will require rapid implementation and expansion during a period of crisis. It cannot burden the user. It must withstand insider attacks.

These are severe requirements. PKI has not been modeled and tested under extremes of this type. It is the security backbone of the future, and must be supported by a vigorous R&D program that addresses its scalability, its extremes, and any vulnerability. It requires the same attention to detail that continuous testing of high-grade cryptographic systems has had over the past several decades.

Malicious Code Detection and Mitigation

The need to nullify malicious code is acute for both the defense information infrastructure and the national information infrastructure because of increased connectivity and reliance on the Internet, increasing prevalence of mobile code, and likely development of and access to code by disgruntled insiders and outsiders.

Malicious code is defined as a program that is written or introduced into a system by someone with malicious intent. The program is intended to damage system function without the operator's knowledge or consent. It is the most rapidly emerging and least understood cyber threat to DoD information systems. Examples of such code are Trojan horses, viruses, worms, trap doors, and time bombs, and each has had notorious successes in worldwide attacks against commercial and military networks and systems. Ominously, the latest versions of these codes represent a merging of the characteristics and capabilities of these existing threats into new, more

powerful forms. Code mobility provided by the World Wide Web has further facilitated the spread of malicious code.

Presently, malicious code is being countered by firewalls, virus-checking software, and similar defensive mechanisms. These mechanisms rely on knowledge of past attack modes. The response to new attacks is reactive, i.e., the response occurs after the attack has been initiated, significant damage to data has been done, and systems have been shut down to cleanse them. Well-designed attacks are succeeding, with such denial-of-service events as Trinoo scripts and "I love you" viruses not only damaging services, but also eroding confidence in the security of both commercial information and the systems required for national defense.

Future research needs to enable malicious code defenses to become more proactive. It must enable real-time detection and neutralization of attacking codes, the development of tolerant system architectures, and the creation of security policies and policy enforcement mechanisms. Though security policy may seem a vague abstraction, it is crucially important in controlling malicious code. Without a security policy that defines what actions are prohibited, it is difficult to argue that any code is malicious and even harder to define policy enforcement mechanisms.

Mitigating and eliminating malicious code in its many forms is crucial for protecting the information infrastructures that are an integral part of our society and the backbone of JV2020. Research for the following areas will require a multi-disciplinary approach that brings together experts from computer science, information security, and real-time systems design. Overarching research needs to be undertaken in the following areas: (1) defining a malicious code taxonomy to facilitate research discussion, (2) providing a mapping between this taxonomy and the kinds of mechanisms that would be needed to protect and detect malicious code, and (3) designing new software architectures and tolerance measures that would facilitate elimination of malicious code. In addition, specific research is required for addressing malicious code, including: (1) semi-automatic source code inspection for existing attacks (static), (2) dynamic code scanning, (3) system integrity checking, (4) reverse engineering, and (5) code signing. This research will broaden coverage of the information assurance spectrum, advance an emerging information assurance industry, and contribute to a deeper understanding of defensive information operations.

Mobile Code Security

Mobile code security decomposes into three challenges:

- Protect hosts from malicious inbound code
- Protect code from malicious hosts
- Construct survivable distributed systems capable of tolerating compromised elements

Although the question of protecting hosts from malicious code is far from resolved, this challenge represents a special case of the general malicious code. The distributed nature of malicious mobile code opens opportunities not available to isolated systems.

Protecting individual parts of mobile code from malicious hosts represents a more difficult problem given natural dependencies on the executing platform. Although general solutions seem distant and speculative at this point, the potential at least bears further exploration.

Conversely, it may be possible to leverage code mobility in constructing survivable distributed systems more capable of tolerating compromised elements. This potential stems from the ability to dynamically distribute an application across many hosts. Such dynamic fragmentation could eliminate a priori information necessary for adversarial strategic targeting. Moreover, if future network bandwidth and computing power facilitate shipping both internal memory structures (e.g., stack) and code snippets around the network, architectures could be constructed with far less exposure at any given time. The challenge of leveraging code mobility to increase survivability seems quite promising as a general area of research.

Anomalous Behavior Detection

The technologies for detecting anomalous behavior are too brittle to produce robust and useable results. Outcomes are laden with false alarms and missed events, both of which increase human and system workload, while reducing confidence in results. These technologies are badly needed for mitigation of the insider threat, as well as for underpinning downstream technologies for detection of related threats.

Fault Tolerance

There is a paradigm-shift taking place in the technical approach to information assurance and defensive information operations. The decades-old approach of resisting attacks and trying to keep all intruders out does not work in the new Internet age. Prevention and avoidance techniques must be augmented with fundamentally secure architectures that can tolerate mobile and malicious code, active content, distributed denial-of-service attacks, and insider threats. We must strive to make systems inherently more tolerant and resilient to attacks, malicious faults, and insider misuse and abuse.

Fault-tolerance technologies have been successfully used to construct highly available and reliable systems for transportation and financial sectors as well as real-time control of plants, vehicles, and command and control systems. Such fault-tolerant systems have been designed to cope with naturally occurring faults and failures such as hardware component faults, design errors in software, and environmentally induced faults such as transients caused by lightning. Advanced research is needed to adapt these technologies for intentional faults and attacks mounted by a human adversary. Research is also needed in creating fundamentally new intrusion- and attack-tolerant systems that use and exploit design diversity, stealth, randomness, and uncertainty as built-in system attributes.

Investment in the following specific technologies is important to achieve the goals of survivable, fault-tolerant systems:

- Proof Carrying Code
- Secure Mobile Code Languages
- System Health Monitors/Tolerance Triggers
- Stealthy System Structures
- Dynamically Reconfigurable System Architectures
- Data Recovery Schemes
- Composability of Trust
- Design and Implementation Diversity
- Uncertainty, Randomness, Agility, and Deception
- Code Execution Real-Time Monitors
- Fragmentation, Redundancy, and Scattering
- Security Policy Specification

High-Speed Encryption

Over-the-network access, both to classified and unclassified-but-sensitive information, is of critical importance, as the Global Information Grid becomes reality. The near-instantaneous global access available once one is "inside" the protected network raises the issue of how to recover quickly from problems such as the loss of an encryption device. There is also the necessity to rapidly add or remove coalition partners from a network during international operations.

For the DoD to conduct operations using the GIG, it must have the ability to almost instantaneously remove selected (compromised) users from the grid, while at the same time permitting the remaining users to continue to conduct their operations. Important pieces of this complex problem are being solved. The STU-III model was a start, but the supporting infrastructure does not scale to required levels. There are upgrades underway, but they are not of the scope necessary to address JV2020 requirements.

At least three major technical challenges exist. First is the development of a high-speed encryption device that can scale to the 10 Gbps rate and beyond. A second challenge is to build an encryption device that is protocol-, algorithm-, and key-agile. This class of device is required if the GIG is to be interoperable with legacy devices and with coalition partners. The third challenge is to reduce the cost of the security functions and to integrate them into embedded capabilities that are transparent to the users. The more transparent the security functions are, the more they will be used and not bypassed in time of crisis. The DoD needs to work with vendors in the earliest stages of developments to integrate highly scaleable security into their products.

Advanced Intrusion Detection/Monitoring

Intrusion-detection technologies currently produce only moderately reliable results in simple environments, and even less-reliable results in complex environments. In terms of correlating and fusing information from distributed sensors in distributed attacks, what little technology exists is too immature to be useful. Intrusion-detection technologies are critically dependent on

monitored sensory data. However, with respect to what is monitored and the places from which the monitoring data are taken, little to nothing is known about either how to decide what should be measured, or how to determine the most effective placement of sensors in an operational environment.

CONSEQUENCE MANAGEMENT

Some network attacks will be successful, and DoD does not have adequate technology in place to address the consequences of the successful attacks. Even as we improve our ability to protect networks and systems from attacks, some attacks will be successful. When a successful attack occurs, we must have tools, techniques, and procedures in place to limit the consequences. The need to continue operations, even at a reduced level, is critical in military operations. Research is needed to improve our ability to address the impacts of successful attacks. Some of the areas that should be included in a research program are self-healing networks and systems, network isolation, integrity restoration, and recovery and reconstruction.

DoD needs to fund research that will allow networks and systems to isolate attacks, gracefully degrade performance if necessary, and automatically heal themselves to a level that will allow users to be confident in using the networks and the information on the networks.

Integrity Restoration

DoD does not have a methodology for restoring integrity in its systems. If a user loses trust in a system, because of an attack (internal or external), or because of a perceived problem, there is a need to validate that the system is performing all functions accurately. Trust in a system can be lost as a result of bad data, natural events, degraded performance, fear of tampering, inconsistent data or decisions, or anything that causes the user to question the usefulness of the system. Tools and methodologies are needed to address system user questions such as:

- Was something done to the system?
- What was done to the system?
- Is the system OK?
- Is the data reliable?

Only if the integrity of the network can be assured to the satisfaction of the user will the system be used as intended.

Recovery and Reconstitution

When a network or system is successfully attacked, there is a need to return it to a useable level of service and ensure that the same attack will not produce the same negative result. Recovery is the process of taking a system from an unacceptable level of performance to a minimum level. Reconstitution is the process of taking a system from the unacceptable or minimum level of performance and returning it to full performance. In addition, the reconstituted system should not be susceptible to fail in the same way from the same attack. The ability to recover and reconstitute a system will increase trust, improve protection against future attacks, and provide systems that have increased availability.

ATTRIBUTION

Once it is determined that a network has been attacked, automated tools are necessary to understand exactly who initiated the attack. Attribution is essential to establish the attacker's motive and to determine an appropriate response.

Observed and reported attacks against DoD computer networks are growing at a rapid rate. As better defense audit tools become available, the number of incident reports will most certainly increase. In general, it is impossible at present to determine the origin and intent of the incident originator. Such incidents could be the result of accidents, curiosity, thrill seeking, intelligence gathering, or deliberate attempts to damage DoD computer networks. The identification of the originator of the incident is one of the pieces of information necessary to scope the response. However, attribution tools are slow at best, are complicated by legal issues, and often fail to reach the masked identity of a skillful attacker.

An extensive R&D program focused on attribution needs to be developed. This is an area where extensive civil, law enforcement, and DoD interaction is essential. Some suggested areas of research include those that follow.

Message Signature Processing

Advanced research is needed to develop algorithms that transform extremely high-bandwidth Internet traffic channels into near-real-time searchable signature spaces such that an attack can be quickly correlated against the passively collected signature stores at multiple nodes. Near-real-time correlation capabilities could narrow the potential set of attributable source points and facilitate rapid engagement of appropriate traps and traces.

Active Code Beacons

Attacks that rely on covert target responses could theoretically be co-opted by the infusion of active code beacons in the return traffic – beacons that would provide attribution information. Research is needed to develop this and other active attribution concepts.

Identification Friend or Foe (IFF) tools

Research in this area would determine if the Identification Friend or Foe concept could be extended to cyberspace to support authentication functions with minimal resource requirements.

CROSS-AREA RESEARCH

There is a broad category of needed R&D that does not fit within the attack phases described earlier, but rather is common to most or all of them. Precisely because of this somewhat non-specific nature, there is much less research being conducted than necessary for the long-term health of the GIG and DoD's overall information infrastructure. In most cases, this R&D lacks a logical "ownership" – it often does not fall clearly within the responsibility of an organization or an industry, and as a result is insufficiently funded.

Below we provide a list of what this Panel believes are the most important areas of research that cut across the attack timelines. Each is discussed in turn.

1. Modeling and Simulation
2. Theory of Vulnerabilities
3. Interdependencies
4. Broad-Based Fundamental Research
5. GIG Research Coordination

MODELING AND SIMULATION

Progress in defending and protecting the GIG will require a far greater ability to model and simulate the performance of information infrastructures than we have today. Currently, much of today's modeling and simulation is based on ad hoc, relatively inaccurate techniques that are specially – and slowly – developed for each specific application. Advanced modeling and simulation techniques will be necessary to characterize and observe the behavior of networks and systems, especially under stressed conditions. Such capabilities will be essential to using an IA test bed effectively. A successfully executed R&D program should result in tools that accurately characterize a wide variety of information infrastructures. Even more advanced versions would allow a rapid, automated way of performing such modeling and simulation exercises.

THEORY OF VULNERABILITIES

Neither system administrators nor commanders can fully rely on today's vulnerability analyses, which are ad hoc, incomplete, unreliable, and unrepeatable. Although some ad hoc analyses can be useful, no theory or associated science exists whereby vulnerabilities can be systematically and completely discovered, assessed, and measured in terms of their effect on operational readiness.

As has been pointed out in earlier studies, one of the most significant gaps in IA research is system-level security engineering, particularly in the area of system-level security architectures. System-level security engineering must be further supported by basic research in IA fundamentals, particularly in the areas of availability and integrity.

INTERDEPENDENCIES

To date there has been very little research into the interdependent effects that can accompany the interconnection of multiple infrastructures, both of the same general type and completely

different ones, e.g., the interdependencies between information networks and the electric power grid. The possibility of cascading and nonlinear effects from such interdependent systems is rhetorically acknowledged but little understood or studied. While responsibility for networks or other infrastructures is often easily identifiable, no organization has an institutional responsibility for interdependent effects. As networks and infrastructures become ever more tightly interconnected, the likelihood and magnitude of such effects will become greater.

This research would seek to understand the nature and origin of interdependent effects and how they propagate between and among infrastructures of varying degrees of complexity. Feedback control theory, network analysis, advanced modeling techniques, and other disciplines would be used in conducting this research, which would seek to assess both intentional (hostile) attacks and naturally occurring instabilities (such as network "storms"). As research progressed, infrastructures with increasing numbers of nodes and interconnections would be studied. At some point, an IA test bed would become an invaluable tool for such analysis.

This research program would seek to shed greater light on the mechanisms and modes of propagation of interdependent effects and suggest technical, management, and policy steps that could serve to both reduce the likelihood of these effects occurring and damp them out once they occur.

BROAD-BASED FUNDAMENTAL RESEARCH

There is relatively little fundamental research on information science, network theory, and network failure. In the private sector, the chief focus is on product development. Private-sector research rarely looks beyond a two-year time horizon. Government and academia have more of a charter to do this kind of research, yet they are not as attuned to needs as is the private sector. At an October 1999 meeting at the White House, the chief technology officers of 15 telecommunications and information technology companies agreed that the private sector had little incentive to conduct such research, although they, along with academia and government, certainly had the necessary resources.

GIG RESEARCH COORDINATION

Management of IA R&D in DoD is fragmented and not focused to meet the rapidly changing threat environment.

The recognition of the GIG as a weapon system calls for a different model for the planning and execution of an IA R&D program to support system implementation. A focused research program will involve academia, industry, and government researchers. Other findings in this report have identified areas where increased funding needs to be applied. This report also points out that the IA environment has changed significantly over the past four years and is likely to change rapidly in the coming years. Such rapid change requires that a flexible R&D plan be developed, one that maintains a balance between near- and long-term problems.

The GIG Executive Office established by the Information Superiority Board (see Architecture Recommendation #1) will develop an R&D plan to execute the additional funding recommended by the DSB.

- The plan will be developed in cooperation with the Under Secretary of Defense Acquisition, Technology and Logistics, the Assistant Secretary of Defense C3I, service laboratories and centers, and appropriate DoD agencies.
- The Information Superiority Board will approve the plan.
- The approved plan will be executed through existing DoD R&D activities (service laboratories and centers, and DoD agencies).

In conjunction with increased research, there is a need to increase the number and quality of people available to conduct IA research. While progress has been made in IA R&D over the last four years, the number of qualified researchers to conduct required research does not meet demand. There is a need to attract more students and faculty in IA research areas. Consistent funding levels and long-term commitments to specific technical thrusts are needed to have a significant impact on the academic community. Qualified researchers will not only allow for increased amounts of research to be performed, but it will also provide a talent pool for industry and government to reduce current projected hiring shortfalls.

COSTS

The Panel was briefed on existing DoD IA and related R&D programs, which were noted earlier. These programs are budgeted at about \$350-400 million per year. Given the major role that the GIG will play in the decade ahead, this figure represents a serious underfunding of a critical defense requirement. The Panel's first compilation of R&D that would make a useful contribution to the IA challenge had a total five-year price tag of \$3-5 billion. A program of this magnitude would not only be fiscally unaffordable, but it would also likely exhaust the human resources available to execute the program. Accordingly, the Panel prioritized the research options and developed three categories of IA R&D programs.

Category 1 R&D is of the highest priority and encompasses R&D that the Panel believes is the minimum that should be added to current efforts to improve the security of the GIG. This R&D category has a five-year estimated cost of \$350 million.

Category 2 R&D is intermediate in priority and is considered important to securing the GIG and providing a sustained basis on which to maintain GIG security well into the future. It has a five-year estimated cost of an additional \$1.2 billion.

Category 3 R&D is lower in priority but would make useful contributions to GIG security and would minimize chances of major vulnerability surprises to both the DoD-unique information infrastructures and the civilian information infrastructures that directly support DoD. It has a five-year estimated cost of an additional \$2.7 billion.

These programs are presented below at their recommended funding levels at each level of funding:

	Category 1 \$(M)	Category 2 \$(M)	Category 3 \$(M)
Scaleable network architectures, sensing, diagnosis:	15	35	80
Malicious code detection and mitigation:	15	30	70
Self-healing networks and systems:	20	65	150
Remediation, recovery, and reconstitution:	30	100	250
Attribution, traceback, forensics, tagging:	25	75	170
Advanced IA modeling and simulation:	30	130	300
Global key management and scalable global access control:	20	55	140
Integrity restoration:	15	50	120
Advanced steganographical techniques:	10	35	80
Metrics research:	10	35	80
Interdependent effects:	15	40	100
Advanced network sensors:	5	25	60
Cyber intelligence tools:	5	35	80
Mobile code security:	10	35	80
Anomalous behavior detection:	5	20	50
Fault-tolerant systems:	15	45	100
High-speed encryption:	40	75	180
Network fault management:	5	20	50
Network isolation:	10	30	60
Electronic friend or foe identification:	5	20	50
Theory of vulnerabilities:	5	20	50
Automated vulnerability assessment tools:	10	20	50
Advanced visualization tools:	5	35	80
Advanced intrusion detection and monitoring:	10	25	60
Attack pattern discovery:	5	35	80
Advanced biometrics research:	0	15	40
Integration tools for coalition warfare:	5	10	50
Research on related societal-issues:	5	35	100

CONCLUSIONS AND RECOMMENDATIONS

The rapid advances in information technology and telecommunications have created a comparably accelerated need for a vigorous, sustained, and balanced program of information assurance R&D. This Panel emphasizes in the strongest possible terms that the IA R&D challenge will be dynamic, growing, and likely never-ending. There are several reasons for this:

- Those who would wish to attack our information infrastructures will constantly be developing new techniques to do so.
- The rapid advances in information and communications technology mean that as the years pass, entirely new infrastructures embodying new technologies will emerge – and each will be accompanied by its own set of new vulnerabilities.
- These new technologies will offer entirely new tools to those who would attack these systems.
- As both current trends and the dictates of complexity theory suggest, systems will become ever more tightly connected and coupled. This will provide new avenues for non-linear and interdependent effects to exhibit themselves, whether through attack or just non-hostile information “storms.”

The Department has been alert to the issues that the IT revolution poses to the composition of future forces. However, the Department is:

- Not addressing its IA R&D personnel requirements with sufficient aggressiveness or creativity, which will likely lead to more serious problems in the next few years as more personnel leave the Department and fewer high-caliber R&D managers remain. Although this topic is addressed more extensively by another Panel report, we believe it is so fundamental that we also need to emphasize the finding. Education and training issues must be among the very first steps that the Department should take in this area. As urgent as other IA technology issues are that we discuss below, this issue is the highest priority in the technology area. Without enough qualified and well-trained technical people, virtually all of the issues in this field that the Department faces will be made much worse.
- Providing insufficient R&D funding to help ensure that the GIG, on which it is placing virtually complete reliance for all future operations, will be secure enough that decision-makers and field commanders will have confidence in the system.
- Managing its current information assurance R&D in a fragmented way that is not sufficiently focused on the information assurance requirements of the GIG. The Department is strongly committed to the Global Information Grid. This commitment requires that those responsible for building and managing the GIG must implement a more robust IA R&D program to assure GIG security in the future.

While the Department's information assurance capabilities are today increasing with time, its dependence upon its information infrastructure is increasing even faster. Unless the Department moves aggressively to address its IA R&D issues, the vulnerability gap will definitely increase.

To strengthen information assurance, the Panel recommends changes to DoD R&D management. Specifically it suggests the following:

- Establishing an information assurance R&D office within OSD that reports to the GIG architect.
- Providing funding of IA R&D *above the current baseline* to this IA R&D office. The actual R&D should then be executed through DARPA, NSA and the service laboratories. Over time, we believe that much of the existing baseline R&D should be shifted to the IA R&D office.
- Providing the IA R&D office with the flexibility to shift some level of funding to meet rapidly emerging threats and vulnerabilities.

Finally, it must be emphasized that these technologies will require *new* investment. Moving resources from minimally-funded protection activities to network restoration activities will not result in an acceptable solution to either problem. Establishing a new milestone of consequence management calls for additional funding. Since the commercial world has largely ignored this issue, solutions will have to start with a vigorous DoD R&D program. This Panel believes that the minimum R&D investment that should be added to current efforts to improve the overall security of the GIG is \$350 million over five years— about twice the level of funding today.

APPENDIX A. PANEL MEMBERS AND GOVERNMENT ADVISORS

Co-Chairs:

Mr. Rich Mendelowitz

General Dynamics

Dr. Robert Mueller

Raytheon Company

Members:

Mr. Bruce MacDonald

Consultant

Dr. Joe Markowitz

Consultant

Dr. Roy Maxion

Carnegie Mellon University

Dr. Dennis Polla

University of Minnesota

Government Advisors:

Dr. Doug Maughan

DARPA/ITO

APPENDIX B. ACRONYMS

CND	Computer Network Defense
DARPA	Defense Advanced Research Projects Agency
DSB	Defense Science Board
GIG	Global Information Grid
IA	Information Assurance
IFF	Identification Friend or Foe
IO	Information Operations
JV2020	Joint Vision 2020
NSA	National Security Agency
OSD	Office of the Secretary of Defense
PKI	Public Key Infrastructure
R&D	Research & Development

ANNEX C

Defense Science Board Task Force on Defensive Information Operations

Panel Report on Organization and Operations

REPORT OF FINDINGS, DISCUSSION/OBSERVATIONS AND RECOMMENDATIONS

TABLE OF CONTENTS

TABLE OF FIGURES	iii
EXECUTIVE SUMMARY	1
INTRODUCTION.....	3
I. Organization and Operations Policy.....	4
II. Resources	11
III. Personnel.....	15
IV. Operational Readiness	23
Conclusion.....	31
APPENDIX A. References	A-1
APPENDIX B. Task Force Members	B-1
APPENDIX C. Policy Matrix	C-1
APPENDIX D. Organization and Operations Panel Questionnaire.....	D-1
APPENDIX E. DIAP Program Development and Integration Team (PDIT) Briefing.....	E-1
APPENDIX F. Acronyms	F-1

TABLE OF FIGURES

Figure 1 - Organization and Operations Panel Focus Areas	3
Figure 2 - OSD-Internal Taxonomy Differences: A Case In Point (IA vs. CIP)	4
Figure 3 - DIO Policy Assessment.....	5
Figure 4 - IO/IA/CIP Organizational Relationships.....	6
Figure 5 – Information Operations Problem Space.....	7

EXECUTIVE SUMMARY

Although the Department of Defense (DoD) has responded to most of the recommendations of the 1996 Defense Science Board (DSB) report¹, progress has been hampered by an incomplete policy framework, insufficient funding, and, most significantly, the fact that the Defensive Information Operations (DIO) challenge has grown more difficult. The goalposts have been moved during the play. The entire DIO landscape continues to be populated with conflicting definitions and policies, unclear roles and responsibilities, and apparent competition among the information operations, information assurance, and critical infrastructure protection (IO/IA/CIP) policy focus areas. The General Accounting Office and DoD Inspector General's office, in several reports² issued since the 1996 DSB report,³ have identified persistent policy and resource issues associated with IA implementation. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) raised the same concern in its *Ninth Assessment of the Information Security Status of Government Systems*.⁴ The Organization and Operations Panel recommends improving this situation by declaring a moratorium on changes to existing IO/IA/CIP-related definitions, while progressing toward agreement on definitions for terms used in common by the DoD and intelligence community, but for which agreed definitions do not now exist. Simultaneously, the panel recommends that specific service- and agency-level policy documents be prepared as required to locally implement aspects of policy established at the Secretary of Defense/Office of the Secretary of Defense (SecDef/OSD) and/or Chairman of the Joint Chiefs of Staff (CJCS) level. The panel recommends the Network Operations (NETOPS) framework be adopted throughout DoD, with Commanders-in-Chief (CINCs), services and agencies collocating their network management and IA/computer network defense operations in the same center. The panel further recommends that the U.S. Space Command be authorized to establish a DoD-wide DIO threat detection and warning capability, using the modified GIG as a technology baseline. This capability should include a feed to the National Operations and Intelligence Watch Officer Network (NOIWON) system. The panel also recommends that a Defense Science Board study be commissioned to specifically address information-attack (cyber) indications and warning.

The panel recognizes that few of the needed improvements cited in this report will come free of cost. However, seen against the value of the underlying equities, the resource requirements identified are small. More to the point, the panel recognizes that military operations and national security, writ large, cannot be successfully prosecuted in the information age without heavy reliance on networked information technologies in public and private hands. Military operations and national security activities must acknowledge and plan for the unintended consequences of commercial infrastructure interdependencies, and networked information technologies must be ever more secure, reliable, and available to meet the full range of foreseeable scenarios and

¹ Defense Science Board, *Information Warfare-Defense* 1996.

² GAO/AIMD-96-84, GAO/AIMD-98-92, GAO/AIMD-99-107, GAO/NSIAO-00-107; DoD IG Reports 99-069, D-2000-058, D-2000-124.

³ Defense Science Board Report, IW-D 1996.

⁴ NSTISSC Report, Feb 2001 (draft).

contingencies. There is simply no other option. The panel recommends that DoD develop a DIO funding strategy and profile, establishing priorities where sufficient funding does not exist; continue to conduct front end assessments (FEA) to shape DIO issues for program and budget decisions; establish a program element (PE) structure for all DIO resources; require mandatory migration of all DoD DIO resources into the new PE structure; address DIO requirements in the Joint Requirements Oversight Council (JROC) (CINC/Service participation); and establish program funding support for DIO requirements. Fully staffed requirements and Planning Program and Budgeting System (PPBS) visibility of all information assurance activities, especially the services' execution of Title X "staff, equip, and train" responsibilities, will greatly assist the U.S. Space Command in planning and executing its more focused and limited operational missions of computer network defense and computer network attack.

The "human face" of DIO is seen through qualitative and quantitative assessment of personnel – military, civilian and contractors – engaged in critical information-protection functions. The panel has identified serious deficiencies in each of these areas, while recognizing that the primary threat to total system security takes the form of trusted – but untrustworthy – insiders. Absent a broad based and sustained effort in the areas of hiring, training, retention, and security, all progress and expense associated with DIO hardware and policy could be for naught. The panel recommends DoD provide recruitment, retention, and proficiency pay for critical DIO skills (authorities exist to do this); develop formal career paths for DIO officer, enlisted, and civilian personnel; develop an outsourcing strategy to complement DoD key DIO resource needs; establish policy to develop and implement formal education training and awareness (ETA) programs for DIO; and require contractor personnel performing outsourced DIO functions to meet ETA criteria required for government employees. Furthermore, the panel recommends that the department strengthen and expand the role of the Reserve Component in DIO by implementing the Reserve Component Study and the DSB Task Force on Human Resources Strategy Study recommendations.

The panel focused primarily on the operational readiness aspects of DIO given its belief that Joint Vision 2020 cannot be achieved without assured access to information. While topics such as policy, personnel, and resourcing are closely related matters of concern, the readiness of joint forces to protect their access to superior information is the prime consideration. Readiness itself can be dissected into issues of metrics, the adequacy and currency of doctrine, rules of engagement, etc. Supporting processes such as red teaming, while addressed in the 1996 DSB report, have not progressed satisfactorily, and existing efforts fall far short of visible needs in this area. The panel recommends DIO be integrated into all operational mission planning to better assure information superiority; DIO be incorporated into formal readiness reporting mechanisms to better measure unit readiness; DIO red teams be formalized and empowered throughout the DoD to stress and evaluate readiness; and computer emergency or incident response teams (CERTs/CIRTs) be established and supported in the department to provide standard alerting and emergency response procedures.

The point is made in the Policy section of the DSB DIO report that national-level policies are deficient in this area. At the same time, policy discontinuities exist both internally in DoD and between DoD and other components of government necessarily engaged in total governmental DIO efforts. Issues of concern in their own right, these unresolved policy debates also stymie efforts to achieve much-needed progress in areas of resource management and training.

INTRODUCTION

The Organization and Operations Panel met between January and August 2000 to review DoD policy, military readiness, organization, training, and resources, and the relationship of each to DIO. Its charter was to examine how the department is organized to execute DIO missions and maintain its readiness for DIO operations.

In the course of conducting this assessment, the Organization and Operations Panel met as a group, received briefings, and considered topics related to its mission, while also participating in task force-wide meetings and discussions. This approach permitted division of effort to focus on the categories of activity listed below. At the same time, it also facilitated identification of cooperative associations between and among issues. An example of the latter would be the relationship between structured readiness reporting by operational units and special-purpose units such as Red Teams. Readiness is measured against defined standards. Red Teams have specific criteria that they operate against which may or may not address those standards, but are a test against a stated level of readiness.], engaged in the level of readiness against defined standards. To provide some background support for proposed recommendations, the Organization and Operations Panel sponsored a DoD questionnaire about Information Assurance (IA) activities to solicit input on issues of concern to the DIO Task Force. The questionnaire results, analysis, and conclusions are provided in Appendix D to this Annex.

The Organization and Operations Panel identified four major categories of findings related to the DoD's execution of the IA/CND/DIO mission areas. These findings are supported by the survey results and are organized into the focus areas enumerated in Figure 1. Discussion of the panel's findings and recommendations follows.

1. Organizational Policy
 - 1.1 Policy and Definitions
 - 1.2 Organizational Roles, Missions, Responsibility Confusion
 - 1.3 Collocation of Network Management and Computer Network Defense Operations
 - 1.4 Threat Warning and Attribution; Indications and Warning
2. Resources and Management
 - 2.1 DIO funding throughout DoD
 - 2.2 Program Element Structure
3. Personnel Issues
 - 3.1 Career Path Management
 - 3.2 Education and Training
 - 3.3 Know Your Insider
 - 3.4 Reserve Component
4. Operational Readiness
 - 4.1 Integration of DIO into mission planning and execution
 - 4.2 Readiness Assessments, Reporting, and Metrics
 - 4.3 Red Teams
 - 4.4 Computer Emergency Response Teams

Figure 1 - Organization and Operations Panel Focus Areas

I. ORGANIZATION AND OPERATIONS POLICY

A. Policy and Definitions (*Internal to DoD and the Intelligence Community*)

FINDINGS: Conflicting definitions and usage related to IO, IA, and CIP within the DoD and Intelligence Community (IC) causes resource and equity fights within the national security community and inhibits progress in resource management, training, and other important areas.

DISCUSSION: This problem exists on several levels. Some DoD/IC definitions and terms are not fungible across government and/or acceptable within the civil sector working cooperatively with government on critical infrastructure protection; those issues and recommendations are found elsewhere in this report.

Traditionally, the Defense Department and intelligence community have worked closely and cooperatively on many issues of great importance to national security. DIO is another issue requiring close inter-working, given the importance of the mission and clear need each organization has for the other in this still-new area. However, in fact, the two are divided by definitional gridlocks that are sometimes subtly nuanced, but behind which lie equity and resource stakes considered important by one or both parties. Some progress has been made in these areas, but many important terms and understandings remain unresolved at present.

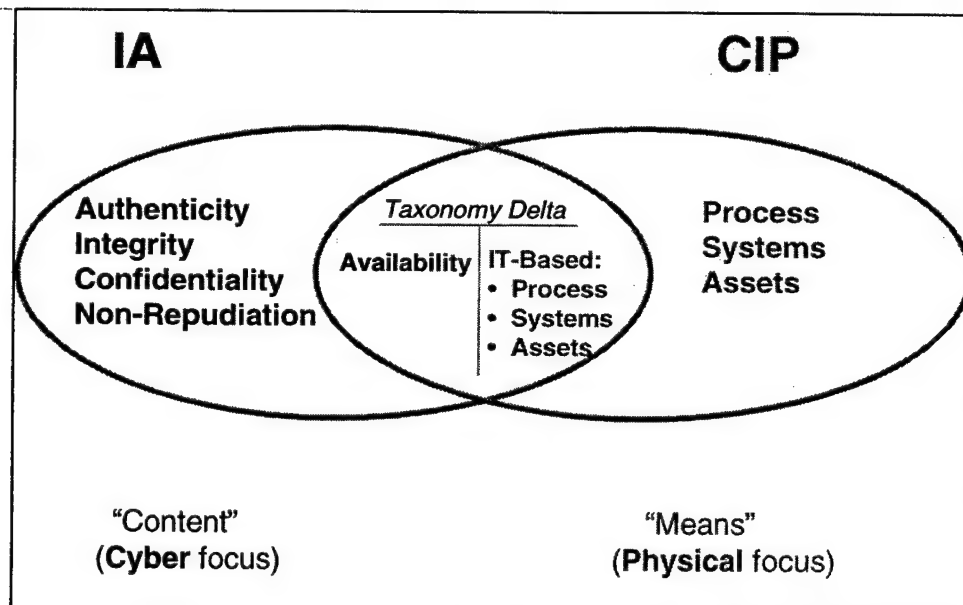


Figure 2 - OSD-Internal Taxonomy Differences: A Case In Point (IA vs. CIP)

At another level, the newness of IO, IA, and CIP within DoD has resulted in tremendous acceleration of the normal evolution of thinking on matters of doctrine, policy, organization, roles and missions, and resource priorities. The frequency with which proposed new approaches to basic definitions and organizational associations have been framed and put forward is matched only by the vehemence of the partisan advocacy for or against any such suggested refinement in

operational procedures or capabilities. If permitted to continue unchecked, the resultant continuous “churning” of the size, shape, and ownership of IO and/or its underlying parts, including IA/CIP/DIO, would significantly handicap broader efforts to inculcate awareness and support for this field within the total force.

Several of the most important aspects of a total DIO management and capability structure are dependent on a relatively stable set of definitions. For example, the goal of providing senior decision makers with the ability to sense, manage and defend “DIO resources” in the aggregate is clearly dependent on a stable understanding of exactly what is included in DIO and what is excluded. Reports that have reached the task force that some resource holders have cynically “redefined” IO to include or exclude certain resources on a case basis are particularly disturbing in this regard.

Training is another area very dependent on a clear and common understanding of basic facts regarding definition, doctrine, authority, and thus roles and missions. Trainees – whether executives or entry-level personnel – all require the benefits of a broadly-based, rigorous, and progressive DIO education, training, and awareness program, as discussed elsewhere in this section of the report. All of them must hope that what they learn will remain valid for some useful period of time.

In order to assess policy for DIO, the panel created a matrix identifying public law, executive orders, national security decision directives, and DoD and other issuances. This matrix is found at Appendix C of this Annex. The extent of the matrix supports the panel's finding that policy formulation and thought development in this area has been both recent and intensive. The panel identified some ninety-five (95) policy documents related to this topic, with fully 39% of them having been authored or updated within the past three years.

Source	Total Number	Number Authored or Updated Within 3 Years	Percent Authored or Updated Within 3 Years
Public Law & Executive Branch Issuances	24	3	13
DoD Issuances	50	24	48
Joint, Agency & NSTISSC Issuances	21	10	48
TOTAL	95	37	39

Figure 3 - DIO Policy Assessment

RECOMMENDATIONS:

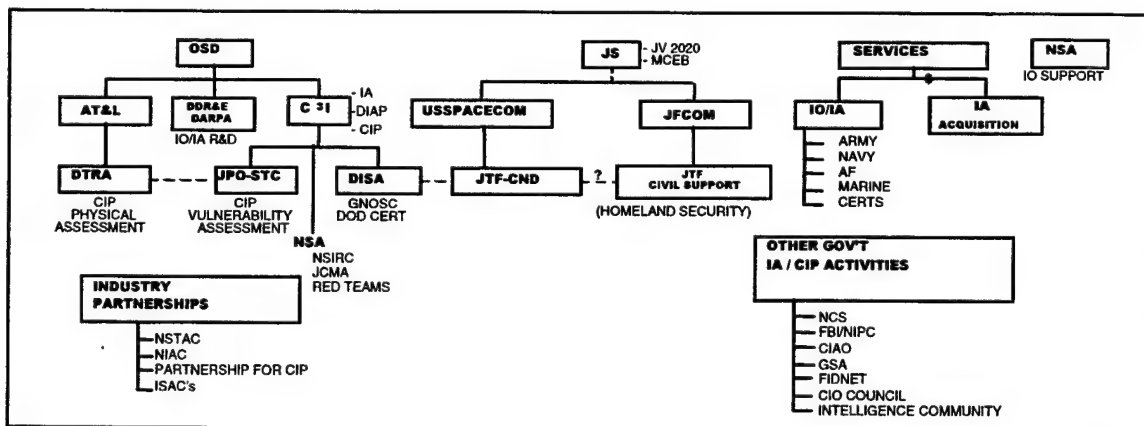
- Deputy Secretary of Defense (DepSecDef) declare a two-year moratorium, effective immediately, on changes to any IO/IA/CIP definitions reflected in joint documents (DoD DIR 3600.1, JP 3-13, etc.). Services and agencies should use this time to

- Leadership of the Bilateral IO Steering Group (BIOSG) Under Secretary of Defense (Policy)(USD(P) and Director, Intelligence Community Management staff) agree to establish, within one year, common/agreed definitions for IO/IA/CIP terms not now resolved in joint documents.
- BIOSG develop and distribute, at the end of the one-year period of resolution, a common lexicon as an aid to facilitating government-wide IO-related definitional commonality.

Estimated cost of implementation: Minimal other than administrative costs.

FINDINGS:

- ### DISCUSSION:



As the concept of DIO has evolved and matured, concerns have been raised about the appropriate roles, missions, and responsibilities of the CINCs, Services, and Agencies in this

area. Recent-real world events and exercises have illustrated that clarification of who is responsible for what activities in DIO is essential. In response, the DoD established the Joint Task Force-Computer Network Defense (JTF-CND) and its component activities in 1998, along with a number of other activities and commands within the military Services to carry out those operational activities deemed necessary for this new mission area. Unfortunately, none of this activity was accompanied by clear policy on who was supposed to do what. Existing policy does not address this mission area, and extrapolation of existing policy has resulted in inconsistent interpretations of roles, missions, and responsibilities across the DoD, as illustrated in Figure 4, above. The department has conducted a number of studies, front end-assessments, and working groups to clarify the issue, but guidance in this area has fallen behind reality. Additionally, where these new missions have been taken on, funding and manpower have been taken out of hide and are inadequate to accomplish what is required. Even where specific responsibilities have been tasked, inadequate resources have hampered the activities' abilities to accomplish taskings. Specific examples of this lack of funding include the Defense-wide Information Assurance Program (DIAP), the JTF-CND, and the Joint Program Office for Special Technology Countermeasures (JPO-STC). None of the activities listed has been funded or staffed appropriately to accomplish its assigned mission.

Another problem arising out of unclear roles, missions, and responsibilities is the distinction between the entirety of DIO, IA, and CND. DIO, as defined in DoD directives and joint publications, includes all activities within IA and some additional activities. CND is an activity within DIO, but is not IA. The relationships among these activities are illustrated in Figure 5, below.

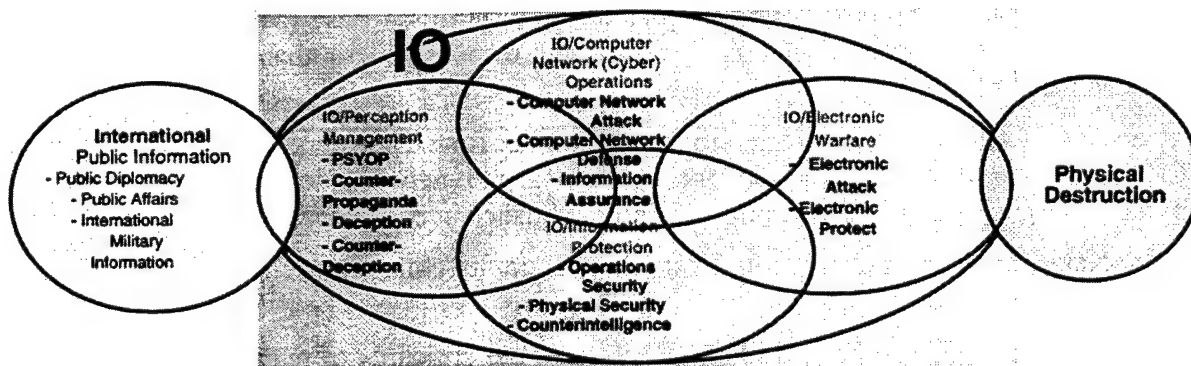


Figure 5 – Information Operations Problem Space

The problem these overlaps in responsibility present is that organizations performing these activities can and do conflict over who is responsible for accomplishing what activity. An example is JTF-CND. Its mission is specifically CND, yet it is not clear what IA responsibilities may or not be included in that mission.

The lack of clarity in roles, missions, and responsibilities has also affected those organizations responsible for carrying out Critical Infrastructure Protection (CIP) activities or homeland defense activities and their relationship to the DIO organizations. Two examples illustrate the problem: (1) the existence of the CIP and DIAP as separate entities within ASD(C3I) and (2) the responsibility of USSPACECOM for Computer Network Defense

(CND)(these are titles and should be capitalized) as opposed to the responsibility of USJFCOM for Homeland Defense when there is a computer network attack against the homeland.

RECOMMENDATIONS:

- SecDef and CJCS clearly define roles, missions, and responsibilities of organizations tasked with DIO functions, including clarifying chains of command and relationships with other organizations.
- When tasking organizations to perform these additional functions, resources should be provided, along with priorities of execution of missions.

Time: To be implemented by October 2001

Estimated cost of implementation: Minimal for definitions. Resources for tasking addressed in separate recommendation.

C. Collocation of Network Management and Computer Network Security

FINDINGS: DoD does not universally collocate its Network Operations Centers with information assurance (IA)/computer network defense (CND) activities.

OBSERVATIONS: Significant operations and security synergy is being realized by the collocation of the DISA Global Network Operations and Security Center (GNOSC) and the Joint Task Force for Computer Network Defense (JTF-CND). The United States Marine Corps (USMC) Network Operations Center at Quantico Marine Corps Base (MCB) is an outstanding example of the efficiencies, security control, and responsiveness that can be provided by collocated network management and IA/CND operations.

USSPACECOM's recent efforts to establish the first Theater C4 Coordination Center (TCCC) with similar potential network operations and network security functionality is a convincing case for similar organizations being established at each CINC headquarters.

The Navy, Air Force, Army, and most agencies do not collocate their network management and security operations.

The Joint Staff Vice J6 briefed the DSB stressing the criticality of realizing NETOPS for the actual operations of the Global Information Grid (GIG).

The DSB was not briefed on, nor is aware of, any DoD initiative to establish an alternate JTF-CND location should the current DISA location be unable to support GNOSC/JTF-CND operations.

The DSB is convinced the NETOPS concept proposed as part of the GIG vision has significant merit and should be adopted throughout DoD – specifically, the collocation of network management and IA/computer network defense operations in the same center.

BACKGROUND: The operation of the network, or NETOPS, is the primary means of operating the GIG. NETOPS meets these needs by means of the standardized organizational and operational integration of three functions: network management, information assurance, and information dissemination management (IDM) (these are all usually referred to as titles).

Network management provides visibility of extent and intensity of activity, traffic load, and throughput potential. Network management will enable dynamic rerouting based on priority, system status, and capacity. The effects of disruptions and intrusions will be minimized through allocation of traffic to unaffected available network paths. Network management will also allow the rapid reconfiguration of networks in order to isolate an incident (e.g., malicious code) to a specific location.

IA is focused on protecting information and information systems. IA provides the organized, manned, trained, and equipped workforce to guard and secure information and information systems. IA incorporates protection, detection, deterrence, and defense capabilities and processes to shield and preserve information and information systems.

RECOMMENDATIONS:

- CINCs, Services, and Agencies take appropriate action to collocate their Network Operations Centers with their comparable IA/Computer Network Defense operations.
- DISA and JTF-CND, in conjunction with U.S. Commander in Chief Space Command (USCINCSpace), determine the optimum alternate location for collocated GNOSC and JTF-CND missions should the current DISA location become combat ineffective..

Time: To be implemented by 1 October 2002

Estimated cost of implementation: \$10-25M over the FYDP

D. Threat Warning and Attribution, "Indications & Warning"

FINDINGS: Recommended improvements in GIG architecture and security provide a technology baseline to permit creation of a tactical time-sensitive, information-attack, warning sensor grid. Such a network would also support goals of assigning attacker attribution confidently and rapidly. Any plan to achieve this outcome would span the domains of policy, law, technology, and organization, and would require actions in several sectors of government, as well as private industry.

DISCUSSION: The recommended actions to secure the GIG architecture, taken together, have the effect of "raising the bar" of protection for DoD information infrastructures. At the same time, however, the panel acknowledges that at least some attacks will succeed in penetrating the security of the GIG. In all cases, there is a need and value in understanding that someone is trying to penetrate and degrade the GIG, even if the attack is not entirely successful. The ability to rapidly, reliably, and confidently identify, characterize, and attribute information attacks against the GIG – and thus, against the nation – is a major national security requirement in the information age.

The recommendations in this report that are related to technology can all be accomplished within the authority of the Secretary of Defense. However, as noted elsewhere in this report, issues related to timely sharing and use of information-attack data are currently unresolved in policy, as they relate to various equities of the federal government. If the scope of interest is expanded to include the extensive commercial infrastructures upon which critical DoD processes

and missions depend, the problem becomes not merely one of policy but also of law, culture, and public sentiment.

If one may presume the availability of timely sensory inputs from GIG-derived sources as a minimum, along with commercial inputs, what remains is to identify the physical and organizational focal point(s) for conduct of an information-attack indications and warning mission, associated personnel requirements, and the chartered authorities and responsibilities those watch-standers would have, including interfaces with larger, classic governmental warning structures.

The I&W Process: Indications and Warning (I&W) is conducted today within a policy framework that assigns roles and responsibilities to a distributed set of organizations throughout the Defense Department and the Intelligence Community.

This structure is well designed to act upon the availability of credible and coherent data, permitting it to "ring the bell," rapidly engaging various authorities to respond as appropriate. However, the problem in the case of information attack is that at present and heretofore, there has been no structured sensory network to reliably provide timely data on which to act.

Precedent may be found in the North American Air (later, Aerospace) Defense Command (NORAD). NORAD is predicated upon an architecture of sensors, reporting links, and analytic nodes, supported by appropriate authorities and focused on a single – but very large, complex, and important – mission: the air defense of the North American continent. The output of the NORAD system is an input into the dissemination architecture displayed and described above.

IMPLEMENTATION: The panel sees the "NORAD model" as a potentially promising approach to information-attack detection, analysis, and warning. Using the upgraded and modified GIG as a sensory baseline, relatively minor modification to the U.S. Space Command's current Computer Network Defense charter and responsibilities would permit identification of an organizational focal point for information-attack threat detection and attack warning within the joint military command structure, feeding the existing NOIWON process as discussed above.

Having established a baseline DoD-internal capability in technology, policy, and organization, the next step will be to expand the information-attack I&W process across the federal government, with the goal a truly national information-protection regime. The information-sharing and trust issues related to this objective are readily acknowledged to be serious and complex, and will have to be addressed [or "treated as such"? treated as such will work] throughout the federal government and across the government-civil interface. The panel immediately acknowledges that the required degree of cooperation is only achievable within a process including extensive discussion and negotiation with private stakeholders; legislative and policy initiative; and continued technological effort, all of which must occur over time. There is cause to be hopeful, however, as the panel has noted the progress being made by such organizations as the National Security Telecommunications Advisory Committee, the Partnership for Critical Infrastructure Security, and other organizations. No specific date targets are established by this panel for the creation of an information-attack I&W regime of national dimensions. However, the requirement is embraced and the vision is put forward, with hope that future study groups and scholars will continue to add specificity and support to this vital initiative in the national interest.

RECOMMENDATIONS:

- SecDef modify the Unified Command Plan as necessary to authorize Commander in Chief, U.S. Space Command (USCINCSpace) to establish a DoD-wide DIO threat detection and warning capability, using the modified GIG as a technology baseline.
- USCINCSpace develop the required capability as a feed to the NOIWON system.
- USD (AT&L) commission a Defense Science Board study to specifically address information-attack indications & warning and make detailed recommendations for implementation of such a program.

Time: Initiate implementation by 1 Oct 2002 and reach Full Operational Capability (FOC) by October 2006.

Estimated cost of implementation: \$150M over the FYDP.

II. RESOURCES

Despite all of the rhetoric and press coverage associated with the threats to and vulnerabilities associated with critical infrastructures, there is scant evidence that the Department has allocated sufficient resources--dollars, people, and leadership--to defensive information operations. *The Report of the President's Commission on Critical Infrastructure Protection*⁵ and the *National Intelligence Estimate on Information Warfare*⁶ both highlighted the growing vulnerabilities to our networks and the evidence that both nation-states and transnational groups are aware of the vulnerabilities and are seeking ways to exploit them asymmetrically. No nation on earth, and certainly no transnational group, can match the U.S. military "bomb-for-bomb" and "bullet-for-bullet"; however, several have the capacity, and apparently the intent, to develop capabilities that can affect our ability to plan and conduct military operations and that touch the lives of ordinary Americans in ways that are physically and economically dangerous. The physical sanctuary that the American people and their military have long enjoyed does not exist in the information age.

A. DIO Funding Throughout DoD

FINDING: The Department has not sufficiently funded protection of its networks and DIO programs. Of particular concern is the Sensitive- but-Unclassified (SBU) information critical to JV 2020. For example:

- Exploding SBU network infrastructures are at risk while pressure increases for more interconnectivity between various security domains and public domains.
- Network interconnectivity in and of itself is causing DoD to invest in non-traditional security initiatives to provide information integrity, electronic identification and authentication, non-repudiation, and availability over and above traditionally funded legacy confidentiality (i.e. Communications Security (COMSEC)) programs

⁵ PCCIP Report, Oct 1997.

⁶ NIE for IW, mmm yyyy.

- The Insider threat is largely ignored, raising trust issues with both SBU and classified networks.
- The looming COMSEC modernization bill to replace aging infrastructure will add further strain on commitment to the SBU problem.

DISCUSSION: In 1996, the DSB recommended funding levels to address deficiencies identified in the Department's DIO budget. Since that time, the funding levels for DIO have increased only slightly in relative dollars, but the requirements and the situation regarding DIO have changed significantly.⁷ In 1996, funding was primarily for classified systems. Subsequently, the Department has realized that its unclassified systems and networks that process sensitive and mission-critical information require protection, but the requirements in this arena have far outstripped the funding available [pick one] to address the problem. Although it may look to the uninformed observer that funding has increased slightly, the reality is that the problem has grown much more comprehensive in scope and funding has failed to keep up with requirements. The result is unfunded mandates and the robbing of critical long-term programs to pay for immediate short-term concerns.

Exacerbating the situation, the DoD has yet to articulate a clear strategy for funding and implementing DIO. There are documents that describe some pieces of a *strategy* (*DoD Chief Information Officer Information Technology Management Strategy*⁸ and the Global Information Grid⁹), but they are incomplete and/or immature and insufficiently detailed to provide a clear picture of the DoD's priorities in this arena. The result of this lack of strategy has been an inconsistent DIO funding profile across the Department, with components making internal decisions about what they can afford regardless of the impact on the overall needs of the DoD. In a shared risk environment, this inconsistent implementation of DIO requirements results in uneven levels of assurance, increasing the risk to all. The lack of an overall strategy, coupled with outdated, incomplete policy, also makes it difficult for the components, and therefore the DoD as an organization, to justify the increased funding levels that they need to address the requirements.

⁷ DIAP PDIT Brief of 14 Jul 2000

⁸ DoD DIO ITM Strategy, Oct 1999)

⁹ DoD CIO P&GM No. 6-8510, 16 Jun 2000.

RECOMMENDATIONS:

OSD should direct the following actions:

- ASD(C3I): Develop DIO funding strategy and profile, establishing priorities where sufficient funding does not exist.
- Conduct front end assessments (FEA) in February 2001 to shape issues for the summer program reviews (PRG) of the 03-08 POMs:
 - DIO Research & Development (R&D) investment: Under Secretary of Defense for Acquisition, Technology & Logistics (USD (AT&L)) lead,
 - COMSEC Modernization: ASD(C3I) lead,
 - CND investment: USCINCSpace lead,
 - GIG implementation investment: ASD(C3I), AT&L, J6 co-leads, and
 - Training/personnel investment: USD(P&R), ASD(C3I) co-leads.

Time: To be implemented by 1 October 2001

Estimated cost of implementation: \$250K contract support to FEAs

B. Program Element Structure

FINDINGS: The current DoD DIO resource management structure hampers effective oversight and executive review.

DISCUSSION: Numerous efforts over the years have attempted to capture, categorize, and manage DIO resources with little success. In the past, DoD captured the bulk of the costs associated with protecting IT resources within its Information Systems Security Program (ISSP). While this program accounted for the bulk of the Department's information security investment, the program does not cover the following information security costs:

- Costs embedded within acquisition programs/initiatives
- Intelligence Community (IC) costs
- Costs within the operating support funds for base/camp/post/stations
- DoD law enforcement (cyber-crime activities) costs
- DARPA information security research programs
- The information security programs of those Agencies not part of the ISSP program (all agencies other than NSA and DISA)

The Defense-wide Information Assurance Program (DIAP) was tasked with the responsibility to provide "oversight, coordination, and integration of the Department's IA resource programs."¹⁰ The DIAP has spent the three years since its inception trying to

¹⁰ OASD(C3I) Memo, 12 Feb 1999.

understand what is and is not included in the ISSP, where additional DIO expenditures within the Department may exist, and how to gain sufficient visibility into these expenditures. The objectives of these efforts have been to understand the scope of the DIO funding and where deficiencies may exist, to provide DoD leadership with the ability to make informed decisions concerning funding. A briefing was given to the DSB DIO Task Force that presented the results of that work (Annex E). It was apparent however, that visibility into DoD components' budgets to determine IA expenditures is still incomplete and the current PE structure does little to correct the problem. The panel's conclusion is that without a Program Element (PE) structure, the ability to accomplish effective management of the DoD's funding resources for DIO will continued to be hampered by lack of visibility.

There are, however, potential negative repercussions that could result from this PE structure and the resulting increase in visibility. The most significant of these repercussions is that DoD components may continue to "hide" DIO expenditures in other funding lines to ensure that they retain flexibility to reallocate internally as conditions dictate. Ensuring that the components retain overall control of their funds, with the understanding that they may receive tasking requirements that they will have to fund somehow, may reduce this activity. Additionally, DoD leadership should refrain from taxing the components' DIO resources during the next Future Year Defense Plan (FYDP) while this key information superiority area is undergoing critical and extensive change. In return, the components need to be honest about the risk management decisions they have made about what to fund and what not to fund and where shortfalls may exist. With that information, DoD has a better chance of justifying additional resources where shortfalls exist.

In addition to establishing a PE structure, DoD needs to ensure that DIO requirements, where appropriate, are vetted and approved through the formal requirements processes. The absence of this step has resulted in unclear priorities on programs and funding, leaving the components to make arbitrary decisions about what they can afford to fund. By vetting through the formal requirements processes, the DIO requirements are both documented and justified, allowing the CINCs who have a major role to play in the actual execution of the DIO mission to have a voice in funding priorities that they currently do not have. Additionally, once the requirements are formally documented, components responsible for funding can be held accountable for decisions made contrary to that requirement – something that is impossible to do under the current situation.

RECOMMENDATIONS:

Director, Program Analysis and Evaluation(PA&E), in concert with ASD(C3I), should effect the following:

- Establish a program element (PE) structure for all DIO resources
- Require mandatory migration of all DoD DIO resources into new PE structure
- Address DIO requirements in the JROC (CINC/Service participation)
- Establish program funding support for DIO requirements

Time: To be implemented by 1 October 2002

Estimated cost of implementation: Total IA budget for DoD should be around \$3B/year, an increase of about \$1.4B over the current documented funding.

III. PERSONNEL

A. Find and Keep the IT Talent

FINDINGS: The DoD shortage of IT professionals is serious and growing.

DISCUSSION: The complexities of solving the DoD shortage of IT professionals, when viewed in the larger context of the private sector, are serious. Shortages in the supply of IT professionals are not confined to the DoD – they exist for other federal agencies, nationally and globally. More than one million information technology jobs are vacant around the world and the number is likely to increase. By 2002, there will be 850,000 vacancies in the United States and more than one million in Europe.

Recruiting is difficult when colleges and universities are only producing enough IT graduates to fill half of the growing annual requirement. Several U.S. companies have begun recruiting foreign nationals to fill their IT jobs. Under the H-1B non-immigrant category of U.S. immigration law, U.S. employers may sponsor 65,000 professional foreign nationals each year. The turnover rate among IT professionals in the private sector is 30%, five times the rate for the private sector as a whole. The private sector is, therefore, providing a number of incentives to combat these shortages.

The Department's ability to compete with the private sector in the area of compensation is limited by personnel practices and guidelines, and by law, in the case of military personnel. The private sector is able to react quickly to any substantive compensation change made in the government, making it difficult to maintain comparability in pay and benefits.], There are a few government authorities that offer limited relief.

The Office of Personnel Management (OPM) authorized specific flexibilities for civilian personnel to help address the government-wide recruiting and retention problems facing managers.¹¹ A recent Integrated Process Team (IPT) within DoD revealed that few of these flexibilities are being used within the Department.¹² Many reasons can be given for this situation, including an unwillingness to differentiate between civilian employees on different types of pay scales, but the most significant reason is lack of funding. As the DoD has sought to reduce its size, the funding for personnel and personnel incentives has also suffered. Instead of targeting reductions to functions that are no longer needed, most activities have taken percentage reductions across the board, exacerbating shortages for key skills.

On the military side, the Services have recognized the need for key IT skills and have begun targeting recruiting and retention bonuses to encourage individuals to remain on active duty. Although these bonuses cannot compare with those offered by the civilian community, they are a tacit recognition of the pay discrepancies. Additionally, other incentives, such as choice-of-duty assignments and DoD schools are used to entice military personnel to remain.

¹¹ "OPM Report, Nov 1998.

¹² IA/IT HR IPT Report, 27 Aug 1999.

Even with adequate incentives, there will be insufficient personnel with specific technical skills available for DoD. This means that a realistic approach to solving the problem must consider outsourcing as an alternative. This approach was explored in some detail by a separate Defense Science Board Task Force on Human Resources Strategy. This DSB recommended pursuing military and DoD civilian tasks only on those tasks essential to the business of governing. All others should be addressed by the private sector for those functions it does best.¹³ This alternative, however, should not be seen as a way to save money, but instead as a method to augment and acquire key IT skills. A Government Accounting Office (GAO) report of August 2000 reports that there are some savings associated with outsourcing, but the documentation of such savings is inadequate.¹⁴ Unfortunately, in the rush to outsource, little thought has been given to careful planning of what should and should not be outsourced. This planning requires a clear statement of "Inherently Governmental" that is understood and executed in a consistent way. Although there is a policy document that describes "Inherently Governmental," the applicability to the IT arena is not clear.¹⁵ There is a current effort to provide this clarification with an Integrated Process Team (IPT) consisting of USD(P&R), USD(AT&L), and ASD(C3I) membership. With this clarification, DoD should develop an outsourcing strategy for key IT skill sets that complement those available from DoD civilian and military personnel.

Other, more creative alternatives should also be considered. It is a well-established fact that IT personnel move around more frequently in their jobs than those in other skill areas. This fact can be a problem for encouraging individuals to take on government service if one expects that the choice is a full career choice. If it is accepted that these frequent moves are part of a valid career choice, then alternative employment programs should be encouraged that facilitate this fluid work force. One alternative may be an "Education and Training for Service (ETS)" model that requires a minimum payback of employment for education. This program could provide dual benefits in encouraging more students to consider an IT career, as well as providing education incentives with a promise of employment. It could also provide a constant refreshment of talent in a constantly changing IT environment.

RECOMMENDATIONS:

- SecDef direct more aggressive recruitment, retention, and proficiency pay for critical DIO skills (authorities exist to do this)
- ASD(C3I), in coordination with USD(P&R), develop formal career paths for DIO officer, enlisted, and civilian personnel
- Develop an outsource strategy to complement DoD key DIO resource needs
- Develop an Education and Training for Service (ETS) model – 3-5 years tenure

Time: To be established by 1 October 2001

Estimated cost of implementation: \$25M per year

¹³ Defense Science Board Report, Feb 2000, p. vii.

¹⁴ GAO/NSIAD-00-107, Aug 2000.

¹⁵ OFPP Policy Letter 92-1, 23 Sep 2000.

B. Sensitize and Train Users

FINDINGS: The DoD workforce at all levels is ill-prepared to execute the DIO mission because current training efforts are fragmented, inadequately scoped, and poorly documented

DISCUSSION: The attacks against the DoD's information infrastructure have heightened awareness of the importance of training in protecting the department's information resources against attacks. Because of the shared risk environment created by highly connected and interdependent information systems, all individuals using, administering, maintaining, and managing systems and networks must understand the threats and the policies, procedures, and equipment designed to mitigate these threats. A training continuum (from cradle to grave, from the lowest civilian and military to the highest) must ensure that all personnel understand the threat and their role in protecting DoD's networks. An analogous program that can provide insight into how training affects successful mission performance is the DoD safety program, particularly aviation safety.

Training for all users of DoD computer systems is mandated by statute,¹⁶ with additional guidance provided by Office of Personnel Management (OPM) regulation,¹⁷ Office of Management & Budget (OMB) circular,¹⁸ and DoD directive.¹⁹ In spite of this direction, user training was unevenly implemented, requiring issuance of additional guidance by ASD(C3I) and USD(P&R) in 1998.²⁰ This policy memo also levied an initial requirement for system administrator and maintainer training and certification. Outside of user training the level and content of training for other personnel with DIO responsibilities (i.e. systems administrators, auditors, accreditors etc) in the Department varies. In some areas there are comprehensive training programs available for all DoD personnel. Unfortunately, the Department does not take full advantage of these programs. In other cases, training has been either unavailable or too expensive for the IA workforce. As a result, the level of training for the DoD IT/IA workforce is uneven at best. The training content also varies across the Department, which is a potentially serious threat to the Department's joint warfighting capability. The previously mentioned policy did not address this issue, nor did it address training for personnel performing other IA functions, or establish a permanent, recurring requirement for those identified functions. That task was taken on by an IPT established in September 1998 by ASD(C3I) and USD(P&R).²¹ This IPT produced a report that made a series of recommendations to begin establishing permanent training and certification requirements for critical IA functions.²² The report resulted in a recently signed DepSecDef policy memo.²³

The Department has made great strides in developing and implementing a DIO training continuum, but much work remains to be done. As the training requirements are developed, they need to not only incorporate the emerging OPM civilian personnel standards and be validated

¹⁶ Public Law 100-235, 1987.

¹⁷ OPM Regulation 5CFR930.301-305, 3 Jan 1992.

¹⁸ OMB Circular A-130, 8 Feb 1996.

¹⁹ DODD 5200.28, 21 Mar 1988.

²⁰ OSD Memo, 29 Jun 1998.

²¹ DepSecDef Memo, 14 Jul 2000.

²² *IA/IT HR IPT Report*, 27 Aug 99.

²³ DepSecDef Memo, 14 Jul 2000.

against commercial/private sector standards (where those exist), but also included in the formal training mechanisms of the Department. Without this formalizing of the requirements into the normal training mechanisms, they will not become institutionalized into how the Department does business. Additionally, it makes little sense to require military and DoD civilians to be trained to a standardized requirement if contractors performing the same functions are not held to those same standards. The recent CIO GIG Guidance & Policy Memo (G&PM) establishes the initial requirement for these training standards.²⁴ Realizing that [this] may require modification to existing contracts, contracting officers need to ensure that any new contracts or modifications to existing contracts providing DIO services/functions contain standardized requirements and performance metrics to hold contractors accountable for meeting these requirements.

RECOMMENDATIONS:

SecDef (ASD(C3I) & USD(P&R), USD(AT&L)) should:

- Establish policy to develop and implement formal education training and awareness (ETA) programs for DIO throughout DoD to do the following:
 - Codify the DIO training program within the formal DoD Joint Training System (JTS)
 - Ensure DIO programs are consistent with commercial and DoD certification standards
 - Require contractor personnel performing outsourced DIO functions to meet ETA criteria required for government employees

Time: To be implemented by 1 Oct 2001

Estimated cost of implementation: \$150M over the FYDP

C. Know Your Insiders

FINDINGS:

- Insiders are our first line of defense and the most dangerous cyber threat
- Systems administrators have the “keys to the kingdom,” yet often require no special “reliability” investigations, such as those in the Personnel Reliability Program

DISCUSSION: The Insider Threat is one that has long been recognized as having the potential to cause the most damage to systems as compared to damage caused by outside attackers— both inside the government and in the private sector. An insider is identified as anyone who “is or has been authorized access to a DoD information system, whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector.”²⁵ An insider has the

²⁴ DoD CIO P&GM No. 6-8510, 16 Jun 2000.

²⁵ Department of Defense, “DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team”. 24 April 2000, p.3

capability to disrupt interconnected DoD information systems, to deny the use of information systems and data to other insiders, and to remove, alter, or destroy information. Documentation of this recognition exists in many fora – including a number of DoD documents that discuss the issue and make recommendations on how to mitigate the risk of the insider. The most comprehensive of these is a recently released report listing the recommendations of the Insider Threat Integrated Process Team, chartered by ASD/C3I.²⁶ This report identifies the basic sources of insider security problems as (1) maliciousness, (2) disdain of security practices, (3) carelessness, and (4) ignorance of security policy, security practices, and proper information system use. The key elements of a strategy to minimize the impact of the insider threat are:

- Establish criticality of systems
- Establish trustworthiness
- Strengthen personnel security and management practices
- Protect information assets
- Detect problems
- React and respond

The report goes on to make a total of 59 recommendations in 7 areas, which, if adopted, will significantly improve the ability of DoD to mitigate the insider threat risk.

A separate report addressing training and certification issues for critical IA functions also makes recommendations to mitigate the insider threat for personnel performing critical IA functions.²⁷ This report specifies that personnel performing critical IA functions – defined as those that require the individual to have privileged access to networks and operating systems – require special attention to ensure that they can be trusted. These critical IA personnel include systems administrators who have the most ability and access to both protect and damage DoD networks. A third report, issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), also addresses the insider threat,²⁸ as does a 1997 DoD IG report.²⁹

There are many ways to address the problem, but all require knowledge of who the critical personnel are, and what the critical processes and systems are. The Y2K effort provides a model of how to distinguish between critical and non-critical systems and processes. The results of this discrimination process can provide a mechanism to focus attention and constrained resources on those systems and processes that are most critical to the Department. However, there is as yet no mechanism to identify critical personnel, although the recommendations by the Information Assurance/Information Technology Human Resources Integrated Process Team (IA/IT HR IPT) begin to accomplish that objective. These recommendations were recently approved by

²⁶ *Insider Threat IPT Final Report, 24 April 2000.*

²⁷ *IA/IT HR IPT Report, 27 Aug 1999.*

²⁸ *NSTISSC Report, Feb 2001(draft).*

²⁹ DoD Office of the Inspector General, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," Report PO 97-049, 25 September 1997

DepSecDef; however, it will take several years just to identify who are systems administrators.³⁰ This step is absolutely essential because systems administrators are the most critical of all those who perform IA functions. Systems administrators can be military personnel who are performing this function in a full-time or part-time capacity, DoD civilian personnel (also full-time or part-time), or contractor personnel performing functions, which have been outsourced. Regardless of their status, all individuals performing these functions must be held to a consistent--and high--standard.

It is not enough, however, to ensure that those performing critical functions are trustworthy, because the most rigorous screening may still miss identifying a potential problem insider. Screening also does not prevent someone who had no intention of misusing the system initially from doing so at a later date. Therefore, monitoring of both personnel and systems must be done to detect those who are not using the system as intended. Such observation requires establishment of a clear, legal, and enforceable monitoring policy so that all personnel using the systems are aware that their activities will be monitored. This policy can also act as a deterrent to anyone who may contemplate unauthorized activity and aid in holding those accountable who violate the policy. The Department has a monitoring policy, but it needs revision to accomplish the objectives stated. The technical means to monitor are available, but require proper configuration and deployment within the network architecture.

Access control processes and mechanisms are also required to prevent individuals from unauthorized access to information and processes. Passwords can provide some measure of control, but require a management process to ensure they are regularly changed. Furthermore, the files need to be protected from disclosure and users need to be aware of their responsibility in protecting passwords. Passwords have their flaws; other access control mechanisms should be employed, such as PKI and biometrics. The DoD PKI program³¹ will address many of the issues presented by access control, and the DSB DIO Task Force applauds this effort. However, deployment could be jeopardized by insufficient funding and lack of follow-up in the enabling of applications for PKI.³² The biometrics program, with the Department of the Army as the executive agent,³³ also shows promise in addressing this issue, but inadequate funding could also jeopardize this program.

The Insider Threat is, therefore, well-documented, and numerous recommendations and programs in several fora exist that, if implemented, would significantly reduce the impact of this threat. However, a number of the recommendations have yet to be implemented. The reasons for this situation vary, but lack of resources and difficulty in developing appropriate policy appear to be the primary factors. This DSB recognizes that the Department has acknowledged the problem, but the lack of policy and resources to address a very real and growing problem is of concern.

³⁰ DepSecDef Memo, 14 Jul 2000.

³¹ ASD(C3I) Memo, 12 Aug 2000.

³² OASD(C3I) DIAP Report Apr 2000.

³³ National Security Act, 1947.

RECOMMENDATIONS:

- ASD/C3I identify those IT personnel who are critical for DIO activities
- DepSecDef mandate the following processes and procedures:
 - System administrator auditing software
 - Open-source, commercial-style background investigations
 - Peer accountability
 - Pre-employment agreements
 - Credit checks
 - Standardized procedures for access to and control of systems
 - Two-person integrity (TPI) for specific critical functions that must be accomplished on a network/system
 - Policy for system monitoring and reporting of improper/unauthorized actions
 - Contractor personnel standards identical to those established for DoD personnel in similar positions

Time: To be implemented by 1 Oct 2001

Estimated cost of implementation: \$5Mper year

D. Reserve Component

FINDING: Significant personnel resource shortfalls affect execution of the DIO mission at all levels in DoD.

The *Reserve Component Study* of February 2000 was chartered to provide recommendations to the ASD(C3I) on the subject of expanding the role of the Reserve Component (RC) in domestic preparedness in two specific areas of defensive information operations: information assurance and computer network defense. The study made two recommendations: 1) bolster RC support for USSPACECOM and JTF-CND, and for the Services by strengthening the RC support to the Service component commands (Land Information Warfare Activity (LIWA), Fleet Information Warfare Command (FIWC) and Air Force Information Warfare Command (AFIWC) and 2) establish Service Joint RC Virtual IA/CND units.³⁴

Virtual RC support to LIWA, FIWC, and AFWIC can provide several advantages. The increase in virtual manning could result in improved mission accomplishment and extended "normal business hours" coverage (the United States' Reserve Components in states encompass six time zones from the east coast to Hawaii); an increase in Service component commands' talent pool (RC members with high technology skills can be reassigned or recruited to perform inactive duty training near home); development of a skilled pool to man the Service component

³⁴ ASD(RA) Study, Feb 2000.

commands during annual training periods of the virtual JWRAC virtual reservists and guardsmen; and an increase in Service component commands' mobilization base. Using the RC in these ways would require little or no addition of on-site staff or facilities. Issues that must be addressed include how to identify reservists with the right skills; the management challenge of virtual drilling; and possible Service reluctance to depend on the RC for full-time support.

Increased RC support to the Service component commands would leverage the expertise of skilled reservists with civilian-acquired skills, capable of conducting virtual operations in support of service missions. The virtual augmentation could perform portions of the service missions that are not completed due to real-world mission pressure or could augment staff during weekends and during summer months.

In addition to the *Reserve Component Study*, there were recommendations made in the *Defense Science Board Task Force on Human Resources Strategy* published February 2000.³⁵ The task force identified a number of priority areas for shaping both the civilian and military workforce, including the Reserve Component: 1) moving to a seamless integration of active and reserve components with a single, integrated personnel and logistics system, and 2) constituting a task force to study and develop a plan that will merge, over time, the Army and Air Force reserve units with their respective National Guards. The report asserts that the transformation is necessary to prevent the personnel problem from worsening.

According to the report, the benefits of integrating these forces include:

- An organization that supports the way the Department operates and deploys
- A more simplified relationship between the active and reserve components
- Reduced overhead from the separate administrative and support structures that exist today
- Stronger ties with U.S. communities

Although the Services have made significant progress towards the goal of full integration, now is the time to leverage that progress by eliminating the separate personnel and logistics structures under which the Reserve Component now operates. Further improvement in the presentation of forces could be achieved by the integration of the reserve force with the National Guard force. This consolidation would require vision and persistence in the face of political pressures, and the challenge would have to be taken up by both the Administration and the Congress.

The DoD increasingly relies on its reserve component to fulfill its mission, both from a resources and skills available standpoint. However, because the two systems remain separate, management of the joint configuration must be relearned each time the reserve component deploys. The report identifies several issues that will have to be addressed to make the integration a reality, including legal, psychological, and administrative hurdles that must be overcome. The report sums it up this way:

The Department should move to a more seamless integration of active and reserve components with a single, integrated personnel and logistics

³⁵ DSB Report, Feb 2000.

*system. The task force recommends that the Secretary of Defense constitute a special task force to make specific recommendations to move toward a single reserve component for the Army and Air Force. However, the task force emphasizes that the move to a more seamless military force should not be delayed awaiting the integration of the reserve components, but should be undertaken as a high priority project under the current active duty and reserve organization.*³⁶

RECOMMENDATION:

- The Deputy Secretary of Defense should direct USD(P&R) and ASD(C3I) to implement
- *Reserve Component Study* recommendations and
 - *Defense Science Board Task Force on Human Resources Strategy* recommendations.

Time: To be implemented by 1 October 2001

Estimated cost of implementation:

- For Reserve Component Study: \$10.5M over the FYDP
- For Human Resources Strategy DSB: as determined by the study, applicable to IT workforce.

IV. OPERATIONAL READINESS

A. DIO Integration into Mission Planning & Execution

FINDINGS: DIO is not adequately integrated into mission planning and execution.

DISCUSSION:

- Control conflicts exist between operational and support equities when services are disrupted.
- Network discipline and CND compliance are issues of concern (e.g., training, standard operating procedures (SOPs), command emphasis).
- Issue of what Components should support the U.S. Space Command's CND mission is still under discussion.
- CINCSPACE should develop a Continuity of Operations Plan (COOP) should JTF-CND lose capabilities.
- It has not yet been determined what CND information should be posted on DOD Global Command and Control System's (GCCS) Common Operational Picture (COP).
- It is not clear what the U.S. Space Command should protect as part of its CND mission beyond the SIPRNET and NIPRNET.

³⁶ Ibid., p. 52.

Integrating DIO into all phases of operational exercises, testing and evaluation, and operational assessments will better ensure that network systems fully consider DIO from design through acquisition and to integration and employment. Implementing DIO into training and plans will ensure that operational plans consider the assuredness of the information they are depending on, and that networks and network personnel are exercised and stressed to better respond when failures and attacks do occur. Planning and exercising for network attacks better prepares the on-scene commanders and operators to respond to attacks or failures in a measured and appropriate manner. Accordingly, as part of exercises and operational plans, developing a set of responses, or delineating the rules of engagement for responding, will ensure any response is appropriate, measured, and authorized.

RECOMMENDATIONS:

- The SecDef, through CJCS, should issue guidance to make DIO a key element of all military planning and operations, to include promulgating Rules of Engagement (ROE) and continuity-of-operations plans and conducting unit training and exercises.

Time: To be implemented by 1 October 2001.

Estimated cost of implementation: Approximately \$500k for initial actions. Additional funding requirements will need to be identified and submitted for funding via the PPBS process.

B. Readiness Assessments, Reporting, and Metrics

FINDINGS: There is no adequate system for assessing DIO readiness across DoD.

DISCUSSION:

- Readiness assessment mechanisms are incomplete and fragmented.
- Numerous efforts are ongoing to measure IA/CND/DIO readiness of DoD activities (e.g., CJCSI 6510.04 and DIAP IA metrics efforts).
- CJCSI 6510.04 does not address or apply to all DoD agencies.
- DoD IA readiness includes assessing, evaluating, and enhancing the readiness posture of DoD IA capabilities.

The success of operational missions is now more than ever dependent on the assured and timely delivery of information from operational commanders to operating forces. Planning for, testing, exercising, protecting, and resourcing the assuredness of those systems that deliver that vital information has not kept pace with the emphasis placed on using the information in some operational manner. Yet, assuring the security and availability of information is critical to DoD's success in peace and war, and is a key element of achieving information superiority. DIO readiness must be measured, assessed, evaluated, and understood for operational commanders to understand and achieve information superiority.

The DoD's information systems have been, and will continue to be, under attack. When disruptions occur to the flow of information, either through attack or system failure, operations suffer.

- System failures are often unpredictable and unavoidable. Network operations reconstitution after a system failure depends on the skill, experience, training, and ability of network technicians.
- System attacks are also often unpredictable and unavoidable. Responses and network reconstitution to network attacks also vary depending on system administrator skill, experience, training, and ability.
- Disabling a network as a response to the threat of attack has the same effect as a successful attack.
- The ability of any given command to better face the challenge of a system failure or attack is improved through planning, training, assessment, and practice.

Policy needs to be established which will lead to a structured, mandated, and recurring DIO assessment capability across all elements of the Global Information Grid. An effective DIO readiness reporting mechanism, accompanied by a viable response mechanism to provide proactive and responsive solutions, is as important as anticipating ammunition shortfalls and assessing more traditional critical warfighting systems, and will in the end save money and conserve other resources. Many different organizations, elements, and activities must be brought together within the DIO readiness system to achieve synergy, efficiency, and effectiveness throughout all facets of the system.

Critical success indicators for the readiness system include the people, operations, training, equipment, infrastructure, and processes that characterize the DIO readiness posture of the DoD described as follows:

- People: The ability to attract and retain qualified, cleared, available, accountable, and motivated personnel to sufficiently staff DIO-related mission requirements
- Operations: The ability of CINCs/Services/Agencies to ensure organizations, procedures, and tools are effectively synchronized to execute DIO actions in order to defend information capabilities; thus providing timely, reliable, integrated, and secure information to achieve mission objectives
- Training: The ability to specify and then satisfy DIO training requirements across the DoD by external and internal education, training, and awareness programs that meet nationally and/or internationally recognized quality and curriculum criteria and that generate qualified and certified DoD DIO work force and users.
- Equipment and Infrastructure: The ability of the DoD's defense-in-depth architecture to ensure authenticated and authorized access to information across service and mission boundaries, throughout all applicable equipment and infrastructures (cyber and physical), and with adequate levels of confidence in information availability, confidentiality, and integrity while being processed, stored, or in transit
- Processes: The ability of the DoD to institutionalize across the Department measurable, repeatable, reliable, valid, cost-effective, streamlined, consistently applied, and well-documented DIO processes

RECOMMENDATIONS:

SecDef, through CJCS, should:

- Promulgate guidance in the Joint Mission Readiness Review (JMRR) and other appropriate Service readiness reporting systems.
- Specify policies to hold commanders accountable for aspects of DIO readiness within their control.

Time: Initial actions by June 2001, with completion not later than June 2002.

Estimated cost of completion: \$12.5M over FYDP

C. Operational Readiness Assessment (Red Teams)

FINDINGS: Due to lack of clear policy and resources, aggressive, comprehensive, effective operational Red Team activities are lacking across DoD.

DISCUSSION:

- Operational readiness assessment involves the Cyber Operations Readiness Triad (CORT): vulnerability assessments, vulnerability evaluations, and red teaming.
- Vulnerability assessments, vulnerability evaluations, and an aggressive, no-notice red-teaming program are lacking across DoD.
- Red-teaming that is being done is inadequately funded, insufficiently staffed, poorly coordinated, and hampered by lack of clear policy.
- Formal Computer Network Attack (CNA) red-teaming efforts, definition, and authorities have yet to be defined.

The purpose of an operational readiness assessment (ORA) is to examine and test an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

The ability of a network system to survive a focused attack and continue to provide the information needed by operational commanders in a timely manner is intrinsically part of information superiority. The ability of any particular system to survive an attack can be attributed to the technical health of the system and the skill, experience, training, and ability of the system technicians. Due to the networked nature of the Global Information Grid (GIG), a weakness within any particular system may cause a vulnerability within the network as a whole.

Evaluating network technical health through testing for system upgrades and patches, proper password management procedures, and firewall standards - just to name a few methods- is necessary to ensure administrators have maintained their systems according to manufacturer updates and established procedures. Similarly, system administrators must be trained and

exercised in recognizing and responding to unauthorized attacks and intrusions, from both within and without of the system. Training and assistance teams provide a vulnerability assessment of networks and help provide the local system administrators with the skills they need to maintain system operations.

The different equipment and software that make up information systems have known and unknown vulnerabilities associated with them. Timely installation and maintenance of manufacturer upgrades and patches for known vulnerabilities helps maintain a higher level of security and assuredness, but often comes after vulnerabilities have been widely known and exploited. This may put operations at risk if the military community does not aggressively test, appraise, and evaluate the hardware and software that makes up the information systems. Evaluations of hardware and software identify vulnerabilities not widely known within the public domain and permit the military to work with developers to correct the vulnerability before hackers can exploit it. This level of evaluation, however, is best done during Research Development Test and Evaluation (RDT&E) and Operational Test and Evaluation (OT&E) so that the best network systems can be acquired that meet the overall DoD information superiority objectives.

Actual readiness of in-place information systems can be measured only through the aggressive testing of a system by an independent (red) team. Red team assessments are conducted throughout the DoD, but often with inadequate resources and limitations placed on their ability to conduct an aggressive assessment. Additionally, red teams are being applied unevenly throughout DoD, which results in some commands being highly effective in thwarting network attacks while others may only have minimal capability in doing so. Also, different red teams evaluate systems using different standards and measures of effectiveness, which may lead to a false sense of security within certain commands. Since a potential aggressor seeks out the most vulnerable system to penetrate or attack to achieve his ends, this uneven approach to red teams may lead to an unrealistic sense of security when in fact, little exists.

It is important for doctrine to be developed that would guide the CORT process to ensure all of DoD is at the same level of DIO readiness. Specifically, red-team structures, authorities, responsibilities, and functions should be specified for all DoD activities, and organized in a manner to make maximum synergistic use of the teams and in-place assets. Accordingly, Operational Readiness Assessment Teams should be aligned for each of the military departments, Defense Threat Reduction Agency (DTRA) for weapons of mass destruction (WMD) purposes, NSA for DoD and national requirements, and Joint Forces Command to organize reserve forces for appropriate missions.

Operational readiness assessments should be conducted often and randomly because any introduction of a new equipment or software upgrade changes the design, and hence the vulnerabilities, of the system. Highest priority should be given to upper echelon command-and-control systems, highly classified systems, and the systems of those forces preparing for operational deployment. But each system within DoD should receive complete CORT assistance not less than every five years.

Because of the nature of networked systems, and DoD's reliance on contractors and vendors, policy should be extended to subject those contractors and vendors who are involved in applicable DoD activities to the same red-teaming standards as DoD.

RECOMMENDATIONS:

Formalize and empower DIO Red Teaming throughout the DoD by:

- Developing a three-level CORT assessment capability:
 - Level I: Vulnerability Assessment (VA)
 - Level II: Vulnerability Evaluation (VE)
 - Level III: DIO Red-Team
- Establishing policy that defines authorities and responsibilities
- Expanding the number, scope, and frequency of Red Teams to include:
 - Once every 3 years for specified LAN-WAN elements
 - As soon as possible after major system/network changes
 - Prior to all force deployments
 - Not less than once every 5 years for all systems and networks
 - That include contractors/vendors to the extent it applies to those government activities
- Providing adequate staffing and resources to accomplish expanded mission
- Reinvigorating and updating draft DoDD 3600.3 to include the CORT process
- Designating NSA as the DoD element responsible for developing tools, tactics, techniques, procedures (TTP), standards, and training to operationalize ORA
- Resourcing NSA to expand its ORA team to meet mission need

Time: 1 October 2001

Estimated cost of implementation: \$30M per year.

D. Computer Emergency Response Teams / Computer Incident Response Teams (CERT/CIRT)

FINDINGS: DoD CERT/CIRT activities vary in their execution and are not inclusive of all DoD CINCs/Services/Agencies (C/S/A).

DISCUSSION:

- Not all Defense agencies have or have access to CERT-/CIRT-like services for their enterprises.
- An overall DIO readiness posture cannot be clearly understood today.
- Tools, response procedures, and reports differ among CERT/CIRTs.
- Doctrine is inconsistent.

CERT/CIRTs provide initial indication of external attack against DoD network systems by using automated monitoring tools to determine when unauthorized probes, scans, intrusions, and service denials occur. The information provided by the CERT/CIRTs permits a clearer understanding of the level, severity, and scope of network attack. This information is also used to alert other DoD network users of attack, and to permit counter measures to be implemented which would mitigate the attack. The sum of all this information is a significant indicator of the readiness and ability of information systems to achieve information superiority.

Today, the various CERT/CIRTs use different tools to monitor network activity and, when suspicious activity is noted, report the information using differing methods and procedures. Further, the tools the CERT/CIRTs use are based on identifying recognizable and known network security vulnerabilities, and are not easily configured to protect against emerging or changing technological threats. These differences and shortcomings mean inequities exist when CERT/CIRTs measure and assess network health, which leads to inefficiencies throughout the system or a false sense of assuredness. For the assessments to be valuable, it is important that they be derived from measurements that are accurate and timely, and able to be dynamically updated to identify and warn against the most up-to-date threats. Additionally, to be easily accessed and understood throughout DoD, the assessments need to have a common format and reporting guidelines.

Because of the nature of their mission, technicians at CERT/CIRTs are particularly adept at understanding and mitigating network vulnerabilities. Therefore, CERT/CIRT technicians provide a critical technical capability and expertise for other commands to draw from when needed, especially in preparation for or during operational employment. However, the current number of CERT/CIRTs and the number of technicians within the CERT/CIRTs, do not adequately meet all the assessment and on-site assistance needs of all CINCs/services/agencies.

RECOMMENDATIONS:

USSPACECOM, supported by OSD/JCS policy and procedure, should improve the DoD CERT structure and scope by:

- Developing doctrine/TTPs on emergency response, including a deployment policy when necessary
- Implementing CERT/CIRT clearinghouse capabilities
- Providing access to standardized and advanced tools and methodologies
- Establishing common reporting formats and a shared common database
- Developing a standardized alerting process
- Establishing additional CERT/CIRTs where needed at C/S/A

Time: To be implemented by 1 October 2001

Estimated cost of implementation: \$50-70M over FYDP

CONCLUSION

The Findings, Discussion and Recommendations described in this report were those that the Panel felt necessary to address the situation and correct deficiencies in organizational and operational issues noted during their investigation of the state of DIO within DoD. A number of activities had been initiated by the Department in response to previous reports (both DSB and others), but were too immature to determine whether the activities would be successful or were actually addressing the identified problems satisfactorily. The strongly held opinion of the majority of the Panel members was that, although there were some technological issues to be addressed in DIO, the majority of the issues impacting the ability of the Department to execute this mission were unclear, conflicting or non-existing policies, non-existing or conflicting operational procedures and inadequate resources. Lack of success in resolving the problems in these areas will continue to hamper the Department irrespective of the availability of technological solutions. The number of activities identified within the Department demonstrates a growing awareness of this fact and the need to develop a solid foundation for action. None of the recommendations mentioned in this report are particularly new or original to the Panel, nor are they difficult to understand or implement with strong, consistent leadership from OSD. That leadership is the key to success.

APPENDIX A. REFERENCES

1. Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) Memo, subj: "Defense-wide Information Assurance Program (DIAP) Implementation Plan", 12 February 1999.
2. Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) Memo, subj: "DoD Information Management (IM) Strategic Plan Version 2.0", 19 October 1999.
<http://www.c3i.osd.mil/org/cio/ciolinks/references/itmstpln/itmstpln-memo.html>
3. Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) Memo, subj: "Department of Defense (DoD) Public Key Infrastructure (PKI)," 12 August 2000. http://www.c3i.osd.mil/org/sio/ia/pki/pki_08122000.pdf
4. Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), *Information Superiority Final Report*, undated (FOUO.)
5. Assistant Secretary of Defense for Reserve Affairs, *Reserve Components Information Assurance Study*, Washington, D.C. February 2000.
<http://www.defenselink.mil/pubs/jrvio2001.pdf>
6. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01B, "Requirements Generation System", 15 April 2001.
http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3170_01b.pdf
7. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3401.01B, "Chairman's Readiness System", 19 June 2000.
http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3401_01b.pdf
8. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3401.02, "Global Status of Resources and Training System", 20 October 1997.(includes Change-1, 19 March 1999.
http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3401_02.pdf
9. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01C, "Information Assurance Implementation (IA Defense in Depth and Computer Network Defense)", draft of 1 August 2000.
10. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.04, "Information Assurance Readiness Metrics," 15 May 2000.
11. Critical Infrastructure Assurance Office, *Practices for Securing Critical Information Assets*, CIAO, Washington, D.C., January 2000.

12. Defense Science Board, *Report of the Defense Science Board Task Force on Information Operations - Defense (IW-D)*, Washington, D.C. November 1996.
<http://cryptome.org/iwd.htm>
13. Defense Science Board, *Report of the Defense Science Board Task Force on Human Resources Strategy*, Washington, D.C. February 2000.
14. Department of Defense, *Report to Congressional Defense Committees: Year 2000 (Y2K) Lessons Learned*, 15 March 2000.
15. Department of Defense Directive 5200.28, "Security of Automated Information Systems
16. (AISs)," 21 March 1988. <http://web7.whs.osd.mil/pdf/d520028p.pdf>
17. Department of Defense Directive 3600.3, "DoD Information Assurance Red Teaming", (draft).
18. Department of Defense Directive 3600.4, "DoD Information Operations Red Teaming (U)", (draft)
19. Department of Defense Directive 5210.42, "Nuclear Weapon Personnel Reliability Program (PRP)", . 8 January 2001 <http://web7.whs.osd.mil/pdf/d521042p.pdf>
20. Department of Defense Insider Threat Integrated Process Team report, *DoD Insider Threat Mitigation: Final Report*, 24 April 2000.
21. Department of Defense, Office of the Inspector General, *DoD Management of Information Assurance Efforts to Protect Automated Information Systems*, Report # PO97-049, 25 September 1997 (FOUO)
22. Department of Defense, Office of the Inspector General, *Summary of Audit Results: DoD Information Assurance Challenges*, Report No. 99-069, Washington, D.C., 22 January 1999. <http://www.dodig.osd.mil/audit/reports/fy99/99-069.pdf>
23. Department of Defense, Office of the Inspector General, *Identification and Authentication Policy*, Report No. D-2000-058, Washington, D.C., 20 December 1999
24. Department of Defense, Office of the Inspector General, *Information Assurance Challenges: A Summary of Audit Results Reported December 1, 1998, through March 31, 2000*, Report No. D-2000-124, Washington, D.C., 15 May 2000 (FOUO).
25. Deputy Secretary of Defense (DepSecDef) Memo, subj: "DoD Chief Information Officer Executive Board", 31 March 2000.
http://www.c3i.osd.mil/org/cio/memo_cio_exec_board3-31-00.pdf

26. Deputy Secretary of Defense (DepSecDef) Memo, subj: "DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001 – March 31, 2000 – Global Information Grid", 31 March 2000. http://www.c3i.osd.mil/org/cio/doc/depsecdememo_gig3-31-00.pdf
27. Deputy Secretary of Defense (DepSecDef) Memo, subj: "Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 'Department of Defense Global Information Grid Information Assurance'," 16 June 2000. <http://www.c3i.osd.mil/org/cio/doc/gigia061600.pdf>
28. Deputy Secretary of Defense (DepSecDef) Memo, subj: "Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification, and Personnel Management in the Department of Defense," 14 July 2000.
29. Deputy Secretary of Defense (DepSecDef) Memo, subj: "Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 12-8430-July 26, 2000 – Acquiring Commercially Available Software", 26 July 2000. <http://www.c3i.osd.mil/org/cio/doc/esio726.pdf>
30. Deputy Secretary of Defense (DepSecDef) Memo, subj: "DoD Chief Information Office (CIO) Guidance and Policy Memorandum No. 4-8460 — Department of Defense Global Information Grid Networks", 24 August 2000. <http://www.c3i.osd.mil/org/cio/doc/gig4-8460-082400.pdf>
31. Deputy Secretary of Defense (DepSecDef) Memo, subj: "DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 10-8460 – Network Operations", . <http://www.c3i.osd.mil/org/cio/doc/gig10-8460-082400.pdf>
32. Information Assurance and Information Technology Human Resources Integrated Process Team Final Report: *Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense*, 27 August 1999. http://www.c3i.osd.mil/org/sio/ia/diap/graphics/Word-IPT_final000827.pdf
33. Information Assurance and Information Technology Human Resources Integrated Process Team Supplemental Report: *Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense*, February 2000. <http://www.c3i.osd.mil/org/sio/ia/diap/graphics/WordIPTSupplementMar17.pdf>
34. General Accounting Office (GAO), *Information Security: Computer Attacks at Department of Defense Post Increasing Risks*, GAO/AIMD-96-84, Washington, D.C., May 1996. <http://www.gao.gov/>
35. General Accounting Office (GAO), *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92, Washington, D.C., September 1998. <http://www.gao.gov/>

36. General Accounting Office (GAO), *DoD Information Security: Serious Weaknesses Continue Place Defense Operations at Risk*, GAO/AIMD-99-107, Washington, D.C. August 1999. <http://www.gao.gov/>
37. General Accounting Office (GAO), *DoD Competitive Sourcing: Savings are Occurring, but Actions are Needed to Improve Accuracy of Savings Estimates*, GAO/NSIAD-00-107, Washington, D.C., August 2000. <http://www.gao.gov/>
38. Information Assurance Technology Analysis Center, *IA Metrics: Critical Review & Technology Assessment (CR/TA) Report*, DTIC, Falls Church, VA, 1 June 2000. <http://iac.dtic.mil/iatac/pdf/Reports/IAMetric.pdf>
39. Joint Pub 1-03.3, *Joint Reporting Structure: Status of Resources and Training System (SORTS)*, Washington, D.C., 10 August 1993.
40. Joint Pub 3-13, *Joint Doctrine for Information Operations*, Washington, D.C., 9 October 1998. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf
41. Joint Chiefs of Staff, *Joint Vision 2020*. <http://www.dtic.mil/jv2020/jvpub2.htm>
42. Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence*, Washington, D.C., 28 February 1994. <http://www.spb.ncr.gov/html/jscrprt.html>
43. Joint Security Commission II, *Report by the Joint Security Commission II*, Washington, D.C., 24 August 1999, (http://www.spb.ncr.gov/doc/JSC_Rpt.pdf).
44. Joint Staff, *Information Assurance: Legal, Regulatory, Policy and Organizational Considerations, 4th Edition*, Washington, D.C., August 1999. <http://www.dtic.mil/jcs/>
45. Keegan, Daniel, "High Tech Work Force Growing", Federal Computer Week, 18 May 2000, <http://www.civic.com/civic/articles/2000/august/civ-cover-08-00.asp>
46. Matthews, William, "IT Workforce counting on contractors", Federal Computer Week, 6 September, 2000, <http://www.fcw.com/fcw/articles/2000/0904/web-survey-09-06-00.asp>
47. Monroe, John Stein. "Work Force Tops CIO's Worries", Federal Computer Week, 9 May 2000, <http://www.fcw.com/civic/articles/2000/0508/web-survey2-05-09-00.asp>
48. National Defense Industrial Association, Command, Control, Communications Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) Committee, *Information Assurance Study*, August 2000.
49. National Intelligence Estimate (NIE) for Information Warfare.

50. National Research Council, Computer Science and Telecommunications Board, *Realizing the Potential of C4I: Fundamental Challenges*, National Academy Press, Washington, D.C., 1999. (http://pompeii.nap.edu/catalog/catalog/cfm?record_id=6457)
51. National Security Telecommunications and Information Systems Security Committee Instruction (NSTISSI) No. 4009, "National Information Systems Security (INFOSEC) Glossary", September 2000. (<http://www.nstissc.gov/Assets/pdf/4009.pdf>)
52. National Security Telecommunications and Information Systems Security Committee report: *Ninth Assessment of the Status of National Security Telecommunications and Information Systems Security within the United States Government*, Washington, D.C. February 2001 (draft).
53. Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I), Infrastructure and Information Assurance Directorate, *Defense-Information Assurance Red Team Methodology*, Mitre Corporation, Washington, D.C. May 1999. (FOUO).
54. Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I), Defense-wide Information Program (DIAP), *Review of Department of Defense Public Key Enabling of Applications for FY 2001-2007*, Washington, D.C., April 2000 (FOUO).
55. Office of Federal Procurement Policy (OFPP) Policy Letter 92-1, "Inherently Governmental Functions", 23 September 1992, <http://www.arnet.gov/Library/OFPP/PolicyLetters/Letters/PL92-1.html>.
56. Office of Management and Budget (OMB) Circular A-130, "*Management of Federal Information Resources*", 8 Feb 1996, (<http://www.Whitehouse.gov/WH/EOP/OMB/html/circulars/a130/a130.html>).
57. Office of Personnel Management (OPM) Regulation 5CFR930.301-305, "Training Requirement for the Computer Security Act," 3 January 1992, (http://www-08.nist.gov/secplcy/opm_plcy.txt).
58. Office of Personnel Management (OPM), *Recruiting and Retaining Information Technology Professionals*, November 1998, (<http://www.opm.gov/y2k/html/recruit1.htm>).
59. President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations*, October 1997.
60. Public Law 100-235, "*Computer Security Act of 1987*."
61. Simpson, Doug, "The Ones That Got Away", Federal Computer Week, 7 Aug 2000, <http://www.civic.com/civic/articles/2000/august/civ-cover-08-00.asp>.

62. Simpson, Doug, "Devising New Lures", Federal Computer Week, 7 Aug 2000, <http://www.fcw.com/civic/articles/2000/august/civ-coverside-08-00.asp>.
63. "The Three Rs of Bonuses and Allowances," FEDweek, <http://www.fedweek.com/NewHotNews/3RsBonusAllow.htm>.
64. Under Secretary of Defense (Personnel and Readiness)/Assistant Secretary of Defense (Command, Control, Communications and Intelligence) Memo, subj: "Information Assurance (IA) Training and Certification," 29 June 1998.
65. U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800-16, *Information Technology Security Training Requirements: A Role-and Performance-Based Model*, Gaithersburg, MD, April 1998, <http://csrc.nist.gov/nistpubs/index.html>.
66. The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0*, Washington, D.C., 2000.

APPENDIX B. PANEL MEMBERS AND GOVERNMENT ADVISORS

Chairman:

Mr. John Grimes

Raytheon Company

Members:

MajGen John Casciano, USAF (Ret)

Litton/TASC

Mr. William Gravell

TRW

LTG Patrick Hughes, USA (Ret)

Private Consultant

Mr. Lowell Thomas

Verizon Communications

Government Advisors:

Mr. Arnold Abraham

OASD (C3I)

CAPT Katharine Burton, USN

OASD (C3I)/DIAP

Mr. Peter Fonash

National Communications System

Mr. Gus Guissanie

OASD (C31)

CAPT Basil Harris, USN

J6K Joint Staff

BrigGen Paul LeBras, USAF

J-2 Joint Staff

LtCol Susan Pardo, USAF

AF/SCMI

APPENDIX C. POLICY MATRIX

Public Law and Executive Branch Issuances					
Public Law	Executive Orders	Presidential Decision Directives	National Security Directives	OMB Circulars	NIST Standards & Guidance
Computer Fraud & Abuse Act (18 USC 1030) 1986	United States Intelligence Activities EO 12333 4 Dec 1981	Security Policy Coordination PDD-29 27 Sep 1994	National Policy for the Security of National Security Telecommunications and Information NSD No. 42 Jul 1990	Management Accountability and Control OMB Circular-123 21 Jul 1995	Information Technology Security Training Requirements NIST Special Publication 800-16 April 1998
Computer Security Act of 1987 (PL 100-235)	National Security Telecommunications Advisory Committee EO 12382 13 Sep 1982	Combating Terrorism PDD-62 22 May 1998		Financial Management Systems OMB Circular-127 Revised 23 Jul 1993	
Government Performance and Results Act of 1993	National Industrial Security Program EO 12829 6 Jan 1993	Critical Infrastructure Protection PDD-63 22 May 1998		Management of Federal Information Resources OMB Circular-A130 Revised 8 Feb 1996	
Paperwork Reduction Act of 1995 (PL 104-13)	U.S. Advisory Council on the NII EO 12864 15 Sep 1993				
Information Technology Management	Classified National Security Information EO 12958 17 Apr 1995				

Public Law and Executive Branch Issuances					
Public Law	Executive Orders	Presidential Decision Directives	National Security Directives	OMB Circulars	NIST Standards & Guidance
Reform Act of 1996 (PL 104-106)					
Security and Freedom Through Encryption Act. (I believe this has never become law.)	Access to Classified Information EO 12968	4 Aug 1995			
	Critical Infrastructure Protection with Amendments	EO 13010	15 Jul 1996		
	Federal Information Technology	EO 13011	17 Jul 1996		
	Administration Of Export Controls On Encryption Products	EO	15 Nov 1996		
	Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet	EO 13035	11 Feb 1997		

DoD ISSUANCES										
8500 - General	8510 - Certification & Accreditation	8520 - Security Management (SMI, PKI, KMI, EKMS)	8530 - Computer Network Defense	8540 - Interconnectivity /Multi-Level Security	8550 - Network/Web (Access, Content, Privileges)	8560 - Assessments (VAP, Red Team, TEMPEST Testing)	8570 - Education, Training, Awareness	8580 - Other	8590 - Critical Infrastructure Protection	Related Information Assurance Issuances
Guidance and Policy for Department of Defense Information Assurance and Guidance Policy Memorandum No. 6-8510 Jan 2000	DoD Information Technology Security Certification and Accreditation Process (DITSCAP) DoDI 5200.40 10 Feb 1998	PKI Roadmap, Version 3 29 Oct 1999	Computer Network Defense DoDD O-8530.aa DRAFT	Secret and Below Initiative (SABI) DoD Memorandum 20 Mar 1997	Policy for Establishing and Maintaining a Publicly Accessible DoD Web Information Service Policy 5215.2 2 Sep 1986 Memorandum 9 Jan 98	Computer Security and Technical Vulnerability Reporting Program (CSTVRP) DoDI 5215.2 2 Sep 1986	Information Assurance Certification DoD Memorandum Jun 1998	Critical Asset Assurance Program (CAAP) DoDD 5160.54 20 Jan 1998	Critical Asset Assurance Program (CAAP) DoDD 5160.54 20 Jan 1998	Unauthorized Disclosure of Classified Information to the Public DoDD 5210.50 27 Feb 1992
Security Requirements for Automated Information Systems DODD 5200.28 21 Mar 1988	DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document DRAFT DoD-M 5200.40-M 21 Apr 1999	Department of Defense (DoD) Public Key Infrastructure (PKI) Policy Memorandum 6 May 1999	Computer Network Defense DoDI O-8530.bb DRAFT	DISN Connection Security Requirements 15 Dec 1999	Information Vulnerability and Web DoD Monitoring and Recording DoDD 4630.6 26 Jun 1981	Communications Security Telephone Monitoring and Recording DoDD 4630.6 26 Jun 1981	Policy on Department of Defense (DoD) Electronic Notice and Consent Banner DoD Memorandum 16 Jan 1997	Critical Asset Assurance Protection DoDD 5160.54 DRAFT	Critical Asset Assurance Protection DoDD 5160.54 DRAFT	DoD Industrial Security Program DoDD 5200.22 8 Dec 1980
Communications Security (COMSEC) (U) 5200.5 Apr 1990	Department of Defense (DoD) Security Certification and Accreditation Process DoDI 5200.40 DRAFT 30 Nov 1999	PKI X.509 Certificate Policy for the U.S. DoD Memorandum 13 Dec 1999	Department of Defense Information Assurance Vulnerability Alert (IAVA) DoD Memorandum 30 Dec 1999	DISN SIPRNet Connection Approval Process, Supplements 1-4 15 Dec 1999	Web Site Administration Policies and Procedures DepSecDef Memorandum 7 Dec 1998					Security Defense Contractor Telecommunications (Includes Change 1) DoDI 5210.74 16 Nov 1996
Security of DoD Contractor Telecommunications 5210.74 Jun 1985	DoD Trusted Computer System Evaluation Criteria DoD 5200.28 STD Dec 1985	PKI Operating Documents Memorandum 13 Dec 1999	DoD Documents DoD Memorandum 13 Dec 1999	Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) OSD Policy Memorandum 22 August 1999	Electronic Newspaper Policy DoDI 5120.4 Policy Memorandum 29 May 1996					Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems DRAFT 28 Feb 2000
Computer Security Evaluation Center DoDD 5215.1, Includes Change 1 Nov 1994		Smart Card Adoption and Implementation Memorandum 10 Nov 1999		DoD	Clearance Procedures for Making Electronic Information Available to the Public DoD Memorandum 17 Feb 1995					DoD Information Security Program DoDD 5200.1 13 Dec 1996

DoD ISSUANCES										
8500 - General	8510 - Certification & Accreditation	8520 - Security Management (SMI, PKI, KMI, EKMS)	8530 - Computer Network Defense	8540 - Interconnectivity /Multi-Level Security	8550 - Network/Web (Access, Content, Privileges)	8560 - Assessments (VAP, Red Team, TEMPEST Testing)	8570 - Education, Training, Awareness	8580 - Other	8590 - Critical Infrastructure Protection	Related Information Assurance Issuances
Control of Compromising Emanations (U) C5200.19 May 1995										
										Information Security Program DoD 5200.1-R 14 Jan 1997
										Personnel Security Program Regulation, Including Change 3 DoD 5200.2-R 23 Feb 1996
										DoD Freedom of Information Act (FOIA) Program DoDD 5400.7 29 Sep 1997
										Control of Compromising Emanations OASD (C3I)
										DoD Technical Architecture Framework for Information Management, Vol 6: DoD Goal Security Architecture Version 3.0 30 Apr 1996
										Electronic Warfare (EW) and C3W Countermeasures DoDD 3222.4 31 Jul 1992
										Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems (C3I) Systems DoDD 4630.5 12 Nov 1992

DoD ISSUANCES										
8500 - General	8510 - Certification & Accreditation	8520 - Security Management (SMI, PKI, KMI, EKMS)	8530 - Computer Network Defense	8540 - Interconnectivity /Multi-Level Security	8550 - Network/Web (Access, Content, Privileges)	8560 - Assessments (VAP, Red Team, TEMPEST Testing)	8570 - Education, Training, Awareness	8580 - Other	8590 - Critical Infrastructure Protection	Related Information Assurance Issuances
										Clearance Procedures for Making Electronic Information Available to the Public DoD Memorandum 17 Nov 1999
										Policy on Operational Test and Evaluation of Information Assurance DoD Memorandum 17 Nov 1999
										DoD Information Operations (U) S3600.1 Dec 1996
										Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection DoDD 5200.39 10 Sep 1997

JOINT, AGENCY, and NSTISSC ISSUANCES				
Joint Staff	DISA	NSA	NSTISSC	DCI
Defensive Information Operations Implementation CJCSI 6510.01B 22 August 1997			National Information Systems Security (INFOSEC) Glossary NSTISSI No. 4009, January 1999 (Revision)	Policy for the Protection of Classified non-SCI Sources and Methods Intelligence (SAMI) DRAFT #21 11 Apr 00

JOINT, AGENCY, and NSTISSC ISSUANCES				
Joint Staff	DISA	NSA	NSTISSC	DCI
			1)	
Defense Information System Network and Connected Systems CJCSI 6211.02A 22 May 1996			National Information Assurance Certification and Accreditation Process (NIACAP) NSTISSI No. 1000 Apr 2000	DCID 6/5T Implementation Manual for the Protection of Classified non-SCI Sources and Methods Intelligence (SAMI) DRAFT #21 11 Apr 00
Policy for the Defense Switched Network CJCSI 6215.01 February 1995			National Training Program for INFOSEC Professionals NSTISSD No. 501 16 November 1992	
Information Operations Condition CM-510-99 10 Mar 1999			Information Systems Security (INFOSEC) Education, Training, and Awareness NSTISSD No. 500 25 February 1993	
Joint Doctrine for Information Operations Joint Pub 3-13 9 Oct 1998			National Training Standard for INFOSEC Professionals NSTISSI No. 4011 20 June 1994	
Information Assurance Implementation (IA Defense in Depth and Computer Network Defense PRELIMINARY DRAFT CJCSI 6510.01C 1 Aug 2000			National Training Standard for Designated Approving Authority (DAA) NSTISSI No. 4012 August 1997	

JOINT, AGENCY, and NSTISSC ISSUANCES				
Joint Staff	DISA	NSA	NSTISSC	DCI
Information Assurance Implementation (IA Defense in Depth and Computer Network Defense PRELIMINARY DRAFT CJCSI 6510.01C 1 Aug 2000				
National Training Standard for System Administrators in Information Systems Security (INFOSEC) NSTISSI No. 4013 August 1997				
Information Assurance (Defense in Depth) Implementation Procedures DRAFT CJCSM 6510.01 1 Sep 2000				
National Training Standard for Information Systems Security Officers (ISSO) NSTISSI No. 4014 August 1997				
Information Assurance Readiness Metrics CJCSI 6510.04 1 May 2000				
National Policy for Incident Response and Vulnerability Reporting for National Security Systems NSTISSP No. 5 Aug 1993				
TEMPEST Countermeasures for Facilities NSTISSI 7000 Nov 1993				

APPENDIX D: ORGANIZATION AND OPERATIONS PANEL QUESTIONNAIRE

1.0 INTRODUCTION

1.1 Organization and Operations Panel Questionnaire

The Organization and Operations Panel of Defense Science Board (DSB) Task Force for Defensive Information Operations (DIO) issued a questionnaire in May of 2000 to assess information assurance (IA) organizational perspectives regarding current Information Assurance functions across DoD. The questionnaire was distributed to 132 organizations, drawn from the Services, CINCs, Agencies and related entities. Each of the selected organizations is currently engaged in IA missions across a wide spectrum of functional areas. The questionnaire sought to elicit information from major IA entities to determine existing roles, mission objectives, organizational relationships, and connectivity as well as to assess the community's self-perceived level of confidence and obtain information regarding perceived needs and future requirements. The results of this questionnaire were also intended to aid in measuring progress toward meeting the specific recommendations of the 1996 DSB DIO report and to develop future policy. The questionnaire presented a series of questions to participants ranging from the identification of each organization's IA missions to the assessment of funding methods for information assurance functions.

The DSB Organization and Operations Panel identified 132 organizations involved in IA activities to represent the DoD IA Community and to serve as the pool of respondents for the questionnaire. Of the 132 organizations that were sent the questionnaire, 56 responded for a response rate of 42%. Table 1 presents the distribution of the respondents by organization type.

Table 1. Questionnaire Response Breakdown

Component	No. of Responses	% Distribution
Services	38	68%
CINCs	5	9%
Agencies and Offices	13	23%
TOTAL	56	100%

The organizations that responded to the questionnaire constituted a broad cross section of overall and IA mission areas and it is therefore possible to extract some general trends from the results.

The initial questions requested the organizations to identify and prioritize both their overall and specific IA missions from the categories below:

OVERALL MISSION OBJECTIVE

Intelligence ☐ C3
Logistics ☐ Plans
Training ☐ Operations
Acquisitions ☐ IG/Audit
☐ Other

FINDINGS:

- 32% of the respondents chose C3 as their overall mission priority
- 30% of the respondents chose "other" operations their overall mission objective
- 14% of the respondents chose IG/Audit as their overall mission objective
- The remaining 24% was relatively equally divided among the remaining categories

FINDINGS

- 31% of the respondents chose management as overall IA mission priority
- 15% of the respondents chose CERT as overall mission priority
- 9% of the respondents chose certification and accreditation as overall mission priority
- The remaining 45% was divided among the remaining categories

OVERALL IA MISSION OBJECTIVE

Certification & Accreditation ☐
Training & Education ☐ Management
☐ Operations ☐ Attack
Characterization Response ☐ ISSE ☐
Systems/Product Acquisition ☐
Computer/Network Crime ☐
Cryptography ☐ Threat Assessment
☐ Vulnerability Assessment ☐ CERT
☐ Web Security
Logistics ☐ Plans

The organizations were also given the opportunity to provide feedback and comments to the DSB with respect to issues of particular concern in the IA arena¹. The comments provide a window into the opinions and concerns of the IA community that was not necessarily consistent with the specific questionnaire responses. These comments appear to suggest that while DoD has succeeded in formulating "high level" policy and guidance with respect to IA issues, the implementation of these policies in the ranks and the development of detailed operational requirements and regulations is an area that must continue to be addressed.

The questionnaire results suggest that the absence of a consistent process to implement IA policy has led to inconsistent actions being taken across the DoD. Many respondents also suggested that policy updates should be issued in a more timely manner, so as to keep pace with technological advances and to avoid the implementation of a patchwork of policy. The questionnaire responses provide a great deal of information and insight into current DoD IA posture, and identify issues that will be of significance in the near term future.

This appendix will provide an analysis of the questionnaire responses and the implied trends throughout the IA community as represented by the pool of questionnaire respondents.

¹ The comments are presented in greater detail in subsequent sections and Attachment A.

1.2 DSB Questionnaire Methodology

Fifty-six organizations responded to the DSB questionnaire. Each organization was treated as an independent entity within the IA community. The analysis, therefore, strives to demonstrate a number of trends present throughout both the IA community and the Department.

The distribution of respondents is heavily Service-oriented and within that group, Army comprised the majority of the responses. However, the trends noted below appear to be consistent across all groups that responded to the questionnaire. Furthermore, the significance of the heavy Service representation is offset by the fact that the Services retain the bulk of the execution responsibilities as delineated by *Goldwater-Nichols*, and so retain primary responsibility for implementing IA programs across the Department. Accordingly, the fact that the Services constitute the bulk of respondents serves to provide an accurate depiction of the composition of the IA community on the ground. This, in turn, lends credence to the purpose of this analysis; namely to provide a window into the current state of the DoD IA community as perceived by the participants. The results also constitute a "pulse check" on the perceived availability of proper resources, policy, and funding throughout the DoD IA community.

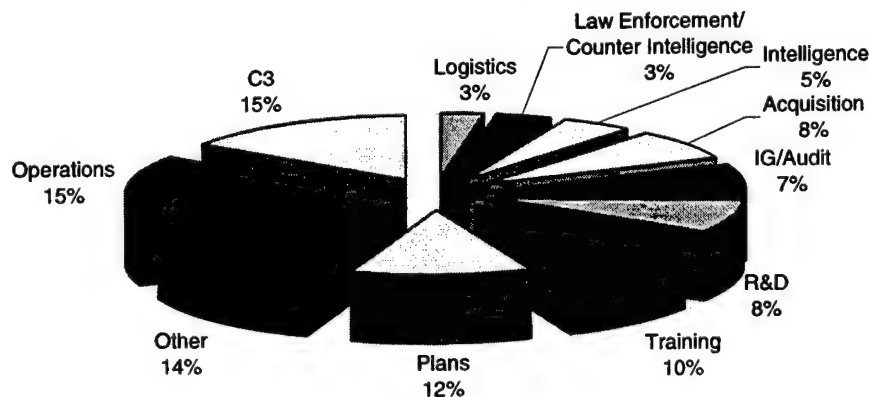
2.0 DSB QUESTIONNAIRE ANALYSIS

2.1 Mission characterization

2.1.1 What is your specific organization's overall mission and overall mission priority?

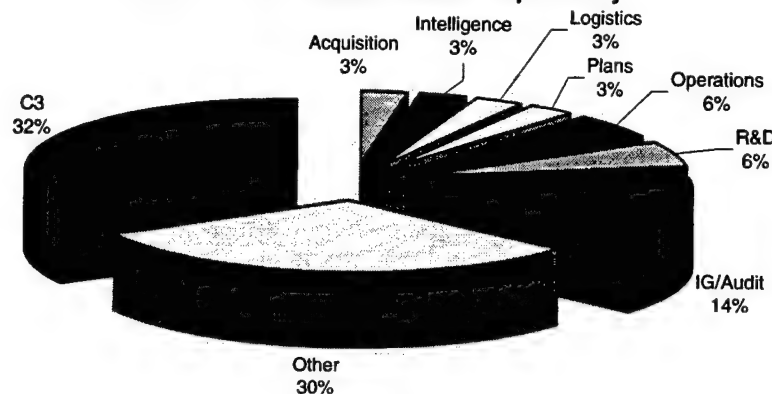
The first question posed in the questionnaire sought to capture the distribution and priority of the overall mission objectives of organizations within the IA community. Respondents were given a list of missions to choose from and requested to select all that applied to their organization. Respondents were then requested to prioritize each mission objective. Figure 1 illustrates the diverse nature of missions within the IA community. On average, each of the 56 respondents chose 2 to 3 mission objectives. Most organizations included C3, operations, and planning among their overall mission objectives.

Figure 1. DoD Overall Mission



The graph illustrates that there is a great deal of variation across the DoD IA community, in terms of mission objectives. As IA continues to gain strength and recognition as a critical element of Defense in Depth, IA issues, and the availability of IA services within the mission areas will continue to grow, placing further pressure on IA organizations for resources, training and other services. Further, while the majority of respondents are involved in C3, planning, training, or some other activity outside of the questionnaire choices, the results suggest that IA activities have become more routine, and an inherent function of DoD business processes.

Figure 2. DoD Overall Mission Top Priority



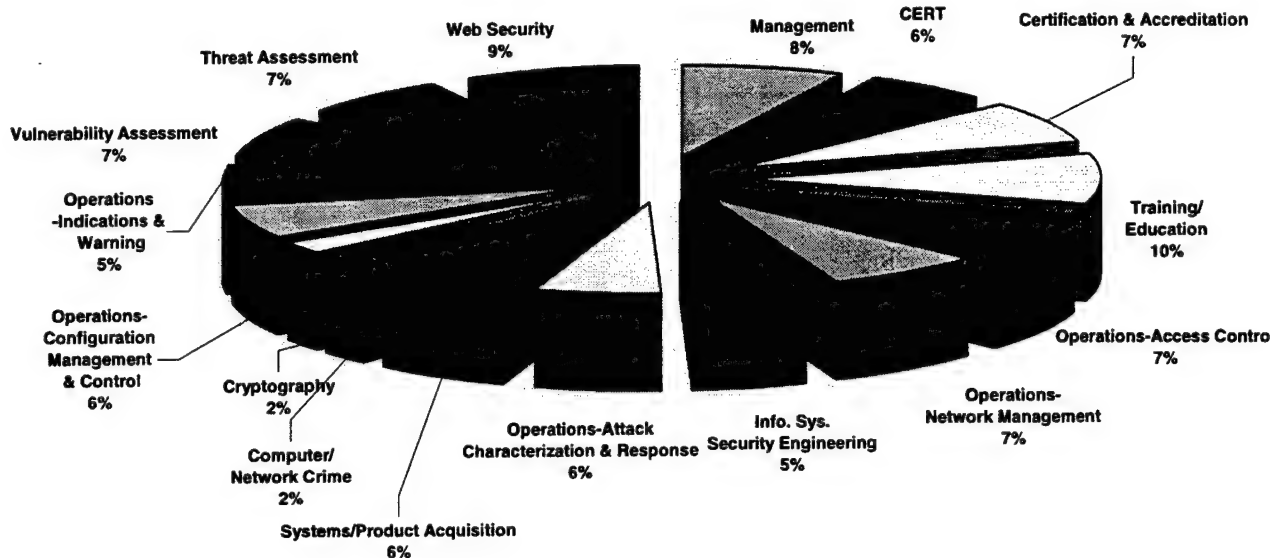
In addition to identifying their mission objectives, respondents were also asked to prioritize their overall mission objectives. Figure 2 illustrates that C3 and IG/Audit were the highest priorities identified by the respondents. The category of "other", which was the choice of a significant number of respondents, suggests that there is a sizable portion of the IA community involved in activities, which have expanded beyond the scope of the traditional mission objective choices. The results seem to suggest that IA is slowly being integrated into the routine of all organizations throughout DoD. Thus, while IA activities continue to be concentrated in organizations with a C3 mission, the results suggest that the IA community is expanding into areas such as R&D and operations.

2.1.2 What is your organization's IA mission and IA mission priority?

Respondents were asked to check and prioritize the overall IA mission objectives that applied to their organization. On average, respondents chose six different objectives from the provided list. Figure 3 illustrates the distribution of the frequency with which each category was chosen.

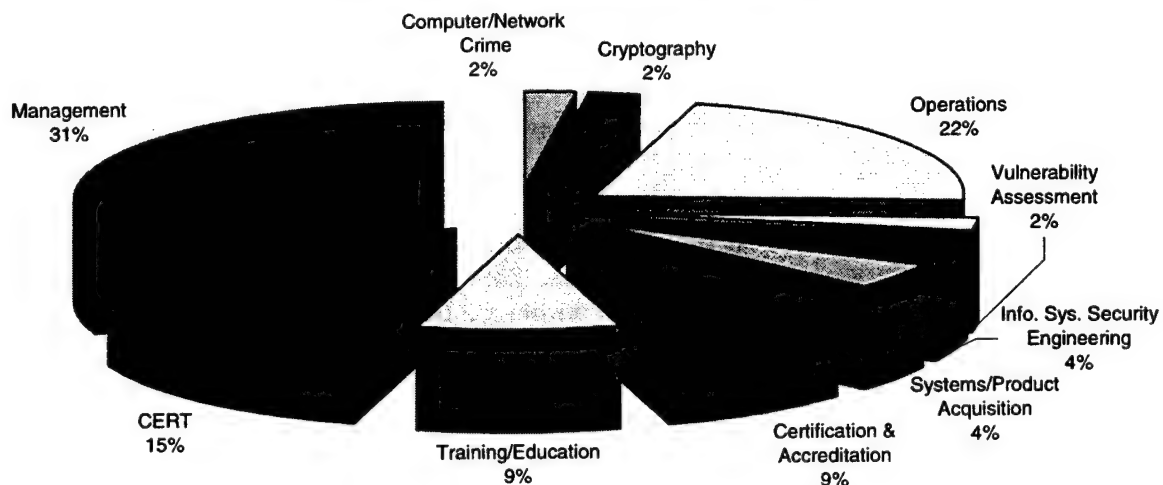
This graph illustrates that the missions of the IA community are quite diverse and cut across numerous focus areas, with training and web security being the most frequently cited IA objectives. The graph further suggests that the IA community's activities are not simply limited to information security issues, but have also become a part of the business processes that exist in the background. IA appears to be developing into a discipline that is increasingly found in a full range of services, suggesting that IA is continuing to evolve into a mainstream activity.

Figure 3. Overall IA Mission
(Respondants were requested to chose all categories that applied)



The questionnaire also asked the respondents to prioritize their overall IA mission objectives. As shown in Figure 4, management was the top IA mission priority chosen by respondents, with nearly one-third of the respondents engaged in some sort of management or oversight role.

Figure 4. DoD IA Mission Priority



Further analysis of the results illustrated in Figure 4 suggests that the IA community has a clear management role, or at least believes it dedicates a great deal of resources towards general management (i.e. accounting, requirements, and funding). The frequency with which respondents chose management as a priority is consistent with the fact that IA is a pervasive issue that reaches almost every organization and activity. As there is a great deal to manage, the infrastructure must be in place to execute all IA activities and initiatives throughout DoD. Management, training, and C&A accounted for 48% of IA priorities, operations as a whole accounted for 22%, CERT accounted for 15%, and general support functions accounted for 13%. However, while these numbers suggest a great deal of variety in terms of the IA priorities throughout the community, it may also indicate that there is divide among the community in terms of mission objective.

2.1.3 Additional observations

In characterizing the IA community's "overall mission objective" and "IA mission objectives", the data suggests that the IA community continues to grow in both scope and in depth. The results also indicate that IA functions are present in a growing number of organizations with a burgeoning variety of overall IA objectives. IA should continue to expand into other organizations and mission objectives as the ability to deliver information in a safe, secure, and highly trusted manner becomes increasingly crucial to the day-to-day operations of the Department. This will be especially true as the Department's E-commerce initiative continues to grow and become standard practice.

2.2 Requirements and Resources

To achieve an overall perspective on the IA community, it is helpful to assess the community's perceptions of its ability to meet the responsibilities set forth in policy both at the departmental and organizational levels. To this end, the questionnaire sought to assess the availability of resources in the form of funding, personnel, and policy.

2.2.1 Have your IA requirements been identified?

Figures 5 through 8 illustrate that the respondents feel that the majority of their requirements have either been fully identified or partially identified, suggesting that they are well able to articulate their IA needs. Almost two-thirds of the respondents have been able to identify their requirements through normal processes, with organizations integrating IA into their standard requests for funding every year. This suggests that there may be sufficient procedures, processes and organizations in place to address IA issues within the PPBS cycle and the POM process.

These graphs also show that about 80% of the community is able to at least partially identify their requirements; however, 42% percent of these requirements have only been partially validated. The relatively large percentage of partially validated requirements implies that it is important to continue to investigate why there is such a substantial amount of requirements that remain only partially identified to facilitate the overall ability of the community to fund its activities.

Figure 5. Requirement Identification Process

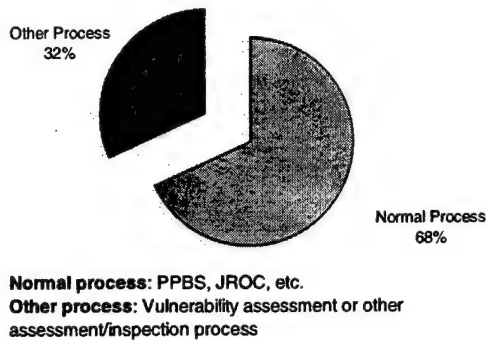


Figure 6. Requirements Identification Using Normal Process

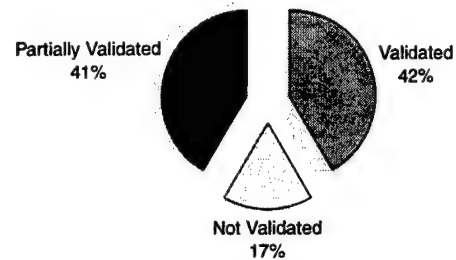


Figure 7. Requirements Identification using Other Processes

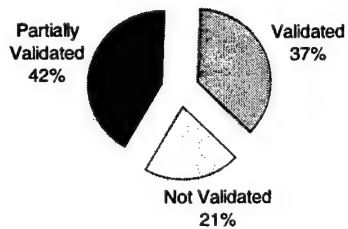
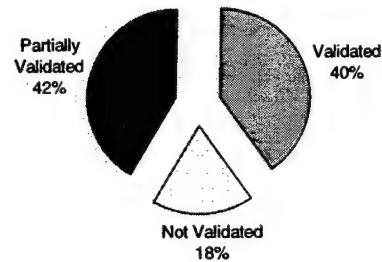


Figure 8. Requirements Identification - Process Independent



2.2.2 Have your IA requirements been resourced?

Figures 9 through 13 illustrate the perceptions among the respondents regarding the effectiveness of their investment and resources.

Figure 9. Do you have enough capital investment funding for IA?

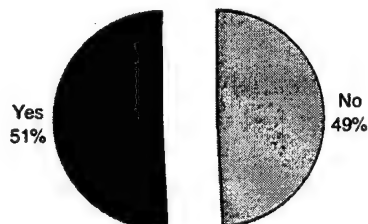


Figure 10. Do you have enough capital investment on facilities?

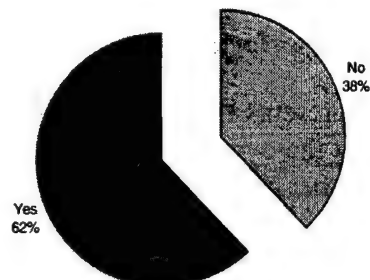


Figure 11. Do you have enough of the right people working IA?

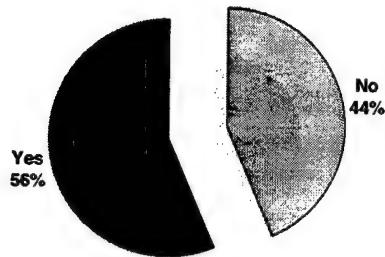


Figure 12. Are your people properly trained?

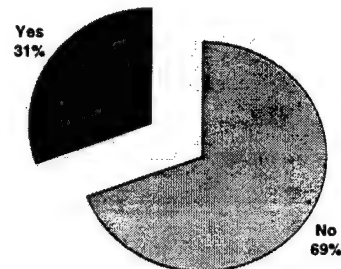
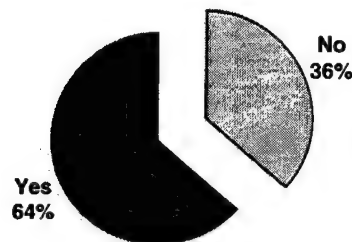


Figure 13. Do you have enough capital investment for IA operations?



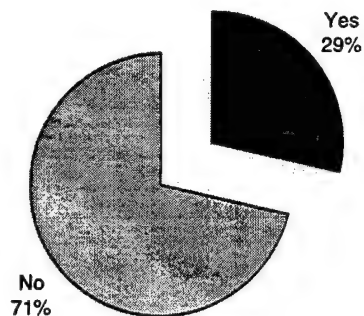
The graphs above illustrate that only about half of the respondents believe they have enough capital investment for IA in general. However, almost two-thirds of the respondents believe they have enough capital investment for facilities and IA operations. This implies that, while the respondents feel that they do not necessarily have enough total resources for IA activities, they feel they are adequately funded for facilities and operations. As almost one-third of the respondents feel they do not have the proper investment capital, further investigation would seem to be warranted.

With regard to personnel requirements, the majority of the respondents felt that they had adequate numbers of people, but that these people do not have the proper training. This correlates to the low placement of education on the IA priority list as seen in Figure 3, and suggests a need to raise the profile of IA education and training throughout the IA community.

2.2.3 Does performance of your IA mission conflict with any other responsibilities?

Figure 14 presents the results from the inquiry regarding potential mission conflict. This figure suggest that the overwhelming majority of respondents do not feel that their IA mission conflicts with their other responsibilities.

Figure 14. Does performance of your IA mission conflict with any of your other responsibilities?



In theory, an organization's IA mission should not conflict with its overall responsibilities because IA is designed to enhance the majority of IA mission objectives engaged in by the community. However, there may be instances when the practical outcome of DoD's IA policy (i.e. smart cards or PKI) may inhibit the tactical world. These services are designed to provide another layer for DoD's Defense-in-depth strategy, yet some organizations may view the additional layers of security as a liability rather than a safeguard.

2.2.4 Do you think you have the right tools to carry out your IA mission?

As a general rule, securing adequate resources in the form of funding or people is a constant challenge for any organization, regardless of the specific issue or technology. However, these issue present only one part of the overall picture. An analysis of the respondent's data implies that, for IA organizations, policy and authority tools are becoming just as important as funding. If Department policy does not clearly communicate the roles and responsibilities that Components are required to implement than it becomes nearly impossible to carry out the IA mission effectively or to cultivate change and growth.

Figures 15 through 17 suggest that while the respondents believe they have generally good information, they do not overwhelmingly believe that the proper policies are in place or that they have the proper authority over subordinates and/or organizations.

Figure 15. Do you think you have adequate and clear IA policy/guidance from above to carry out your IA mission?

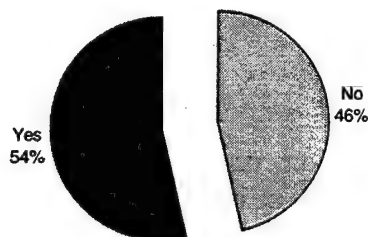


Figure 16. Do you think you have adequate authority over subordinates/organizations to carry out your IA mission?

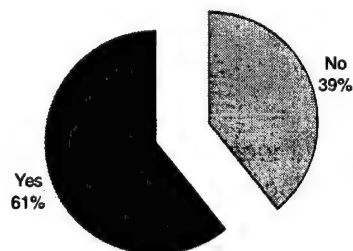
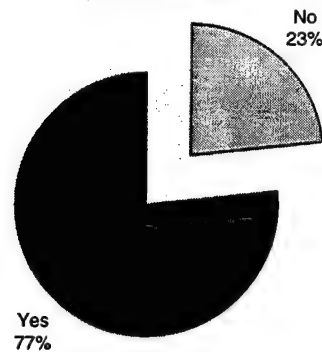


Figure 17. Do you have adequate information you execute your IA mission?



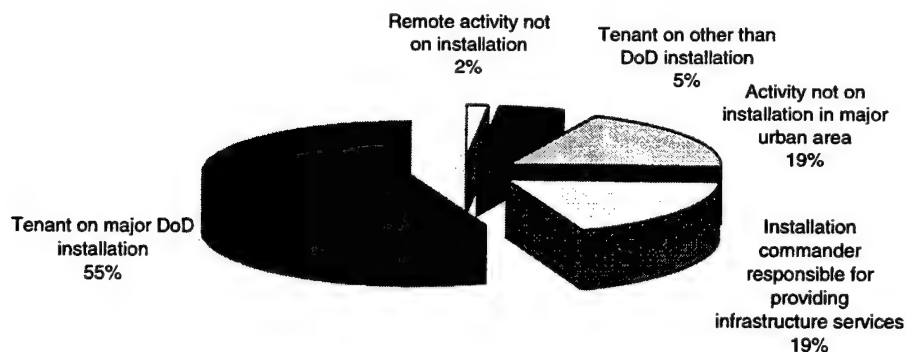
This becomes especially important in the case of Agencies and CINCs who are often dependent on the Services for the delivery of IA services. The results also point to the growing interdependence of organizations in the IA community that has developed as a result of information sharing and enhanced communication within the community.

2.3 Infrastructure Availability

2.3.1 Activity Situation

Figure 18 illustrates that the majority of DoD IA activities sit on major DoD installations.

Figure 18. What best describes your activity situation?

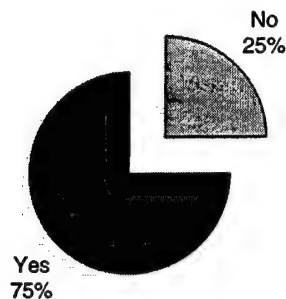


The second most common situation is activities where the installation commander is responsible for delivering infrastructure services. These may be minor installation or installations in an urban area. An additional twenty- percent of the respondents are situated in remote locations.

2.3.2 Availability of DoD Infrastructure

Figure 19 addresses the availability of essential infrastructure.

Figure 19. Do you consider DoD Infrastructure services in mission planning?



The results of this question illustrate that about three-fourths of the respondents consider the DoD infrastructure in mission planning. This suggests that organizations are considering both information assurance and infrastructure assurance issues, which have a symbiotic relationship. Without the availability of the various elements of the DOD infrastructure, it becomes difficult if not impossible to meaningfully execute the IA mission.

Figure 20. How do you consider DoD Infrastructure availability in mission planning?

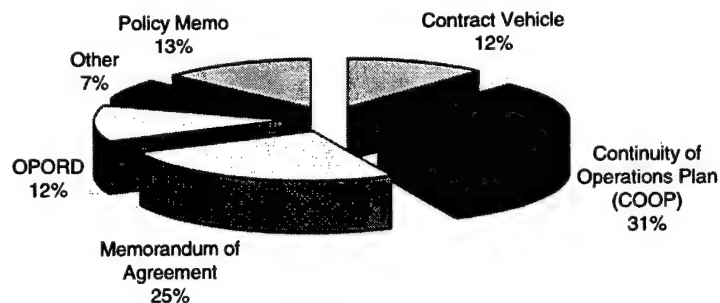


Figure 20 suggests that most respondents consider DoD infrastructure for Continuity of Operations Plans (COOPs) and for memoranda of agreement (MOA). Since the availability of the infrastructure drives COOPs and plays a key role in MOAs, it is not surprising that the respondents chose these two most frequently. In addition to assessing those situations where

organizations consider infrastructure issues, it is also important to ascertain the level of an organization's confidence in the availability of infrastructure at critical times.

Figure 21. Are you confidence in that the services you require will be available whenever needed?

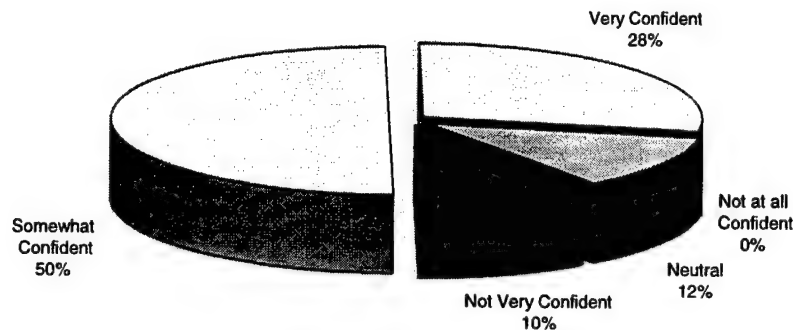


Figure 21 illustrates that only about one quarter of the respondents are confident that the infrastructure services upon which they rely will be available whenever needed, while over 50% of the respondents are only somewhat confident that the services they need will always be available. Such results suggest that there is a pronounced absence of confidence in the current ability of the DoD infrastructure to deliver services on demand.

2.4 Impact of IA Activities on Mission Performance

2.4.1 How do the following IA processes impact your mission performance?

Figures 22 through 28 illustrate the impact of IA activities on mission objectives.

Figure 22. Vulnerability Alert Process

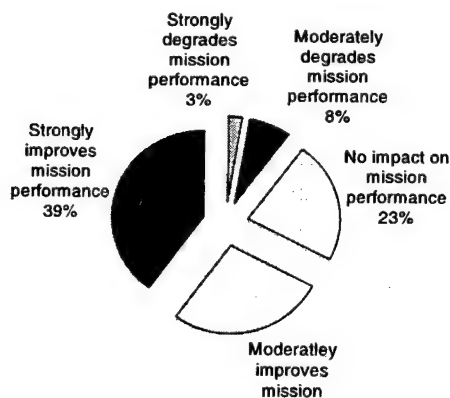


Figure 23. INFOCONS

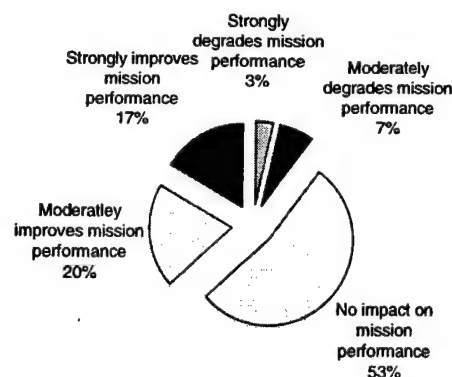


Figure 25. Accreditation Process

Figure 24. Incident Reporting Process

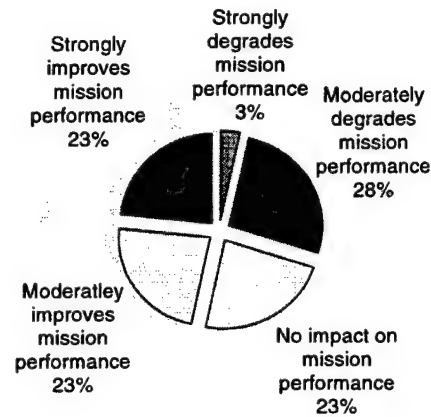
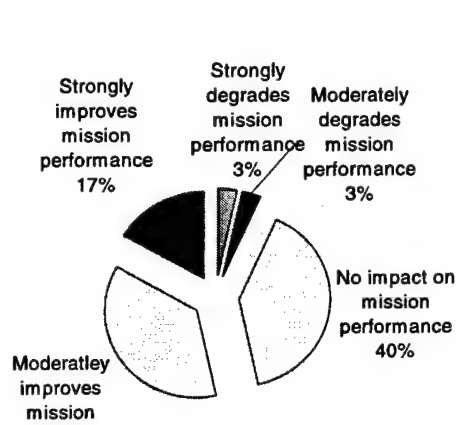
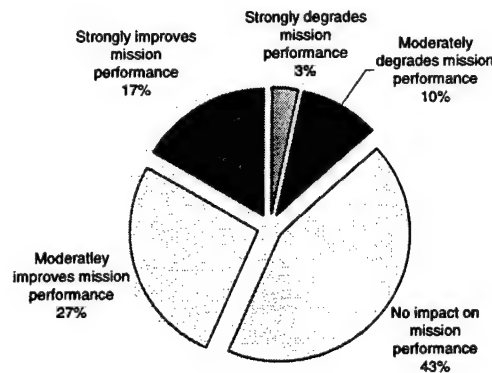
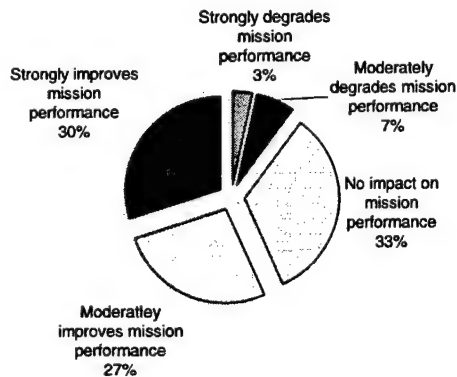


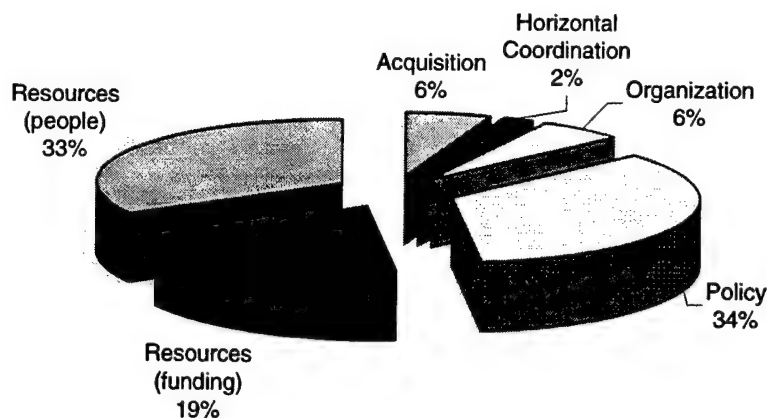
Figure 26. Vulnerability Assessment Process

Figure 28. Recovery/Reconstitution Process



The results suggest that Vulnerability Alert Process and Vulnerability Assessment most significantly influence the respondents' mission objectives. Most of the IA activities have only very little or a moderate impact at all on mission. While virtually no IA activities have a strongly negative impact on mission objectives, threat assessment and the accreditation and certification activate moderately degrade mission performance, with respondents reporting that about one-third of the these activities were at least moderately degrading mission objective.

Figure 29. Issues Warranting Attention



2.5. Issues Warranting Attention

While IA has made significant progress in expanding its reach throughout the Department, there are still a variety of issues that must continuously be examined and reevaluated. As with any program or initiative, funding and well-trained personnel will always be issues to program managers. Perhaps the most interesting result of the questionnaire analysis is the fact that policy was identified as the single biggest concern of the respondents. These results were borne out by the "Comments" received at the end of the questionnaire and presented in full in Attachment A.

The small numbers for acquisition, organization, and horizontal coordination suggest that communication among organizations is adequate and that the organizational structure of the IA community itself is not of great concern. However, issues such as roles and responsibilities as well as new money allocated for various IA efforts continue to challenge the organizations that are charged with implementing the changes. The concerns reflected in Figure 29 are consistent with the trend found throughout the questionnaire indicating that the community is generally confused, and in need of a greater guidance as well as policy that has more detail and applicability to their own organization's day-to-day functions.

2.6. Coordination and Interface

Respondents were asked to provide insight into the organizations they work with and draw support from in both the public and private sectors. Please see Attachment B for the results of this inquiry (i.e., a full list of organization's coordination and interface from questions 10a, 10b, and 10c).

3.0 COMMENTS

In addition to the specific data represented in the graphs set forth in the previous sections, organizations were also asked to provide more general feedback on those issues not specifically covered by the questionnaire. These comments were intended to give participants the opportunity to highlight any areas of particular concern in the IA community with respect to the subject matter of the survey, and to provide the DSB with greater insight into those concerns. A frequent focus of these concerns is the expressed need for clear policy, and resources, both with respect to funding and qualified people. While many organizations responded positively to the specific survey questions directed towards the adequacy of policy and guidance, respondents' true feelings about their IA posture was clarified in the comments, and presents a somewhat less sanguine view of the state of policy at the organizational level. . This apparent discrepancy between the comments and the specific survey responses may be indicative of a desire on the part of the respondents to provide a "politically correct" response to the direct questions in the survey.

A detailed review of the comments seems to indicate that most organizations would welcome clearer policy and guidance from OSD, which would enable them to better develop policy specifically applicable to their own organizations. Many of the respondents expressed the belief that there was sufficient be "high level" policy", however, this policy was of limited use when applied to the organizational structures of the community, and their day-to-day tasks. The comments further suggest that efforts on the part of policy makers to clarify roles and responsibilities at the organizational level to facilitate the implementation of IA initiatives would be well received, as would requests for suggestions about the process at the operational level. The comments also indicated that that a lack of "low level" policy was leading to the creation of multiple concurrent and possibly inconsistent policies with respect to the delineation of varying roles and responsibilities. It was suggested that such situations should and could be addressed by undertaking a more comprehensive and wide-ranging policy effort. A related undercurrent in the comments, was the expressed desire for the IA community to begin to think and act across organizational lines and to coordinate efforts and hare information.

Respondents also suggested that policy formulation difficulties might stem from the incremental nature by which DoD develops IA policy. Which contributes to the "patchwork" of policies currently in use. This policy "incrementalism" is perceived as a barrier to timely updates, which would allow policy to keep pace with developments in technology.

Many respondents expressed the belief that the visibility of IA in the PPBS cycle must be raised in order to assure that resourcing priorities are adequately addressed in the FYDP. These funding needs are further complicated by the great diversity of IA mission objectives as represented by the survey respondents. Respondents also expressed a desire to see further discussion in order to identify activities that support multiple missions and to harness domain knowledge in support of further policy and program development and implementation. This process will be invaluable in overcoming the inherent limitations of the PPBS too allow for the full identification and validation of IA requirements in the future.

A final area of concern was the IAVA and accreditation processes. There was a general consensus that the feedback and reporting loop on the IAVA process needs to be tightened, leading to better and more timely communication. Additionally, many respondents felt that the accreditation process was both too complex, and too "paper intensive", leading to delays and frustration.

Overall, the comments indicate that the IA community is beginning to view itself as a functional community that cuts across organizational lines. There is also a high level of awareness of the fact that many of the organizations are dependent on each other, as well as outside institutions, and, a broad sense of the need for better coordination and cooperation in the IA community.

4.0 CONCLUSION

The responses received to the questionnaire came from a broad cross section of IA organizations engaged across the full spectrum of IA missions. The respondents accurately reflect those organizations and components, which are charged with the primary responsibility of implementing IA programs across the DoD. The questionnaire results support the proposition that IA is becoming instantiated across all functional areas of DoD, and that while high level policy is adequate, significant work remains to be done to assure that the broad goals and objectives of DoD policy are accurately translated into usable policies at the operational level. Front line IA personnel must be provided with sufficient organizational tools and resources to competently implement their IA missions on a day to day basis. Furthermore, policy must keep pace with technology, developed and implemented in a consistent manner across the various organizations that comprise the IA community. This becomes especially crucial as the demand for IA services continues to evolve into an important element of each Component's activities.

Attachment A: Noted Trends in Respondents' Comments

Unclear and Outdated Guidance from Above

We write the IA policy for the AF, however, we do not always get clear policy/guidance from OSD.

There is too much policy that is not related to performing the functions required to do the job. The problem is the incremental adding of policy over the years. We need to throw it all out and start over.

DA IA Policy needs further clarification on roles and responsibilities. Typical, rapid technology change places us in the position of not always having desired information on hand for decisions.

Adequate & clear IA policy/guidance from above - NO - as an example, there is still no clear authoritative reporting policy from JCS on IA incidents.

There are various policies out there but the focus is still at the highest (DOD) levels. The personnel putting these policies into action, need more clarity to carry out this mission.

Although large strides are being made in regard to IA/CND policies, policy is not keeping up with the speed of technology. A paradigm shift is necessary to ensure that security policy is addressed in a more timely manner.

Policy is still being formulated from the national level on down. It seems to be mile wide and inch deep. Much improvement has been made in the last two years.

Several IA policy documents are old/out of date (e.g. DODD 5200.28, Public Law 100-235, DOD 5200.28-STD (Orange Book), etc).

IA policy which addresses Certification and Accreditation (DODI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP)) is difficult to understand and use. It expanded the process via required steps and paperwork, with vague guidance. Recommend Interim Authority to Operate be allowed at completion of Phase I vice Phase III.

Question 6: IA policy between DoD and the separate services sometimes parallels or conflicts, particularly in locations where there are multiple policy makers.

Little Authority over Subordinates/Organizations

Have NO authority over service component organizations - they have their own reporting lines - the Title 10 issue all over again.

As a CINC who must respond for their respective Components, we have little say when the reporting structure and infrastructure is based upon a Service-centric model. That's why we face difficulties with the real C2 of the networks, as evidenced with disparities in INFOCON levels, as just one example.

The IA organization at DSS has no real authority over subordinates/organization. IA's role is more an advisory/oversight function without true authority to control systems or system owners.

Limited Financial Resources

We are not funded adequately for that protection to be maximized to the extent necessary to protect our infrastructure. Our CO is very supportive but funding limits and sets our priorities.

NCIS is currently not funded for this mission. We have made extraordinary strides in meeting this challenge, which are not being replicated within DoD, and are maximizing the limited resources we have.

While there is guidance from above with respect to IA policy/guidance, limited resources constrain programs to a (illegible) that could be deemed unacceptable. There are several DoD mandates that DSS is not in compliance with.

A strong commitment of "resources" and "will" is required by leadership at all levels to be the warfighter's IA agency of choice!

Limited Human Resources

Finding qualified people is difficult, more so on the GS side than on the contractor side.

Accreditation is a big obstacle for us because we have so many systems and so few people.

Suggestions for Change

IA should be budgeted as a separate program to ensure you get the required resources (personnel, training and tools).

I recommend having an area IA assigned to an IG area that provides full time support and overwatch to all IG offices within a pre-determined geographic location / area support. Responsibility for all IG offices within the assigned sector or geographic locations.

Attachment B: Organization's Coordination and Interface

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
Air Force	AFCIC	All Air Staff functionals; OSD, Joint Staff, NSA, DISA, DIA, IC, Army, Navy, USMC, MAJOR COMMANDS, JTF-CND, CINCs, NSTISSC.	Various government contractors	All of the above.
Army	DAIG	None.	None.	DAIG, V Corps, 3d Corps Support Command
Army	Office of Inspector General-West Point	DAIG, DoDIG, OSC	None	DAIG, DoDIG, OSC
Army	n/a	JCAHO (Joint Commission on Accreditation of Healthcare Organizations)	Japanese Healthcare System, US Healthcare Insurance Firs	TIMPO (Tri-Service Information Management Program Office), DoD Health Affairs, USAMISSA, TMSCC
Army	DISC-4	NSA, DISA, ASD C3I, DCSPS, DCSINT, CECOM, ISEC, NSSTISIC	ISS, STS, Sytec, GSA, Mitre	NSA, CECOM, ISEC
Army	n/a		NAI, ISS, Harris Corp Smartforce	
Army	DISC-4	Assistant Secretary of Defense for C3I, National Security Agency, Defense Information Systems Agency, US Air Force, US Navy, US Marine Corps, Defense Intelligence Agency, General Services Agency, National Institute of Standards and Technology, Joint Staff		National Security Agency, National Institute of Standards and Technology, Defense Information Systems Agency, Joint Staff
Army	n/a	DISA CID, MI (CI), NSA	CERT (Carnegie Mellon)	MI, NIPC, JICPAC (USCINCPAC), DISA
Army	Space and Information Superiority Directorate		MPRI; Mitre; TAMSCO; COLEMAN Research and others	TRADOC Schools and Centers; CECOM; DISC4; DISA; ARL/SLAD; ATEC; and others

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
Army	n/a	Microsoft and other software vendors.	Services and Products contractors	Microsoft, DISA Cert, ACERT
Army	n/a	USAFE, NAVEUR, DISA, DISC4, ASC, EUCOM, NATO, CND JTF, LIWA ACERT-CC, 202nd MP Group (CID)	Cisco, ISS, Network Associates, Symantec, Microsoft	Army Signal Command, DISC4, EUCOM, USAF, NAVEUR, USAREUR, LIWA, DAMO-ODI
Army	Field Operations	DISC4, PEO STAMIS, PEO GCSS, PEO AMD, PEO AVIATION, PEO IEW&S, CECOM, DARPA, LIWA, ASC, NSA,	IEEE, SANS, AFCEA,	All of the above
Army	n/a	Members of Federal CIO Council, and subordinate offices of the members.	Most any company in the US.	ASD(C3I), DoD Defense Information Assurance Program.
Army	SAF/IG	INS, Official Passport Office, DFAS-Charleston and Denver ETC.		7th ATC, USAREUR and DAIG
Army	n/a	ANSOC, ACERT, CIAC, MEDCOM, TRICARE, OSD HA, ANSOC	NORTH AND MCAFEE, GOVERNMENT COMPUTER NEWS, FEDERAL COMPUTER WEEK, INFORMATION SECURITY, CHIPS	ACERT, MEDCOM, OSD HA, CIAC, TRICARE, NARMC MEDDACS
Army	SAF/IG			
Army	DISC4		Vendors providing IA products and services	DoD ASD C3I, CECOM, ARL, ASC, LIWA
Army	n/a	EUCOM, DISA, USAF, MARFOR-Europe, NAVFOR-Europe, ACERT	None	EUCOM, DISA, USAF, MARFOR-Europe, NAVFOR-Europe, ACERT, Army RCERTs, AFWIC, SHADOW
Army	RCERT-E		ISS	ARIN, RIPE
Army	n/a	congress (rarely), FBI, CIA, NSA	Sun Systems, MicroSoft	too far down the org. to respond
Army	n/a	U.S. Air Force, U.S. Navy,	Microsoft, Remedy,	ACERT,
Army	n/a	VA	numerous contractors	MEDCOM
Army	DAIG	White House, Congress, Justice Department,	Various vendors (Microsoft, CISCO, 3COM, etc.)	DISA, ANSOC, DISC4 and installation DOIMs
Army	SAF/IG			DAIG IRMD Fort Campbell DOIM
Army	DISC4		We interface on a routine basis with vendors. Many vendors are selling their products. Other vendors hold IA tool contracts.	NSA for EAL standards -- Army CERT - Army Signal Command (ASC) theater Network Operation Centers (NOC) -- Army Regional CERTs -- JTF-CND.

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
Army	n/a	NIST, NAVCIRT, AFCIRT, NSA, DISA, ARMY DOIM, ARMY PORTAL, CIO IA TEAM, USAPA, USASC IASE, DTIC	Computer Science Institute, SAN, MICROSOFT, ISC2, Rootshell, ICSA, IEBT	Computer Science Institute, SAN MICROSOFT, Rootshell, security focus, whitehats, antionline
Army	SAM	Defense Information Systems Agency (DISA), Air Force Pentagon Communications Agency (AFPCA), Army Information Management Support Center (IMCEN), Office of the Secretary of Defense, Information Technology Directorate (OSD/ITD), Department of the Navy, Info	Major Network Vendors, i.e., Cisco, Cabletron, Alcatel, etc., Major Information Technology Consultants, i.e., Gartner Group, MITRE, etc.	Defense Information Systems Agency (DISA), Air Force Pentagon Communications Agency (AFPCA), Army Information Management Support Center (IMCEN), Office of the Secretary of Defense, Information Technology Directorate (OSD/ITD), Department of the Navy, Info
Army	SAF/IG			
BMDO	OSD/BMDO	DTRA, DARPA, ARMY, NAVY, Air Force, Marine Corps, DISA, DIAP, OSD (A&T), OSD(C3I), Air Force Office of Special Investigations, Army 902nd Military Intelligence, NSWC Dahlgren, foreign security offices for some programs	IETF, ASIS, and AFCEA	All the ones we interface with are in some ways supporting us.
DISA	DISA	OSD, Joint Staff, CINCs, Services, Agencies, Law Enforcement, Intel Community, NATO, NCS academia	IT community in general and IT community in general and academia	MITRE, ROME Labs, DARPA, Lawrence Livermore, Carnegie Mellon, NSIRC, NIST
DISA	DISA-EUR- RCERT	Regional CERTS in the EUROM AOR IA representatives from the components in the AOR, EUROM IA division	Training organizations	HQ DISA
DISA	n/a	NSA, ALL CINCs, GAO	EDS, SAIC, CSC	NSA
DISA	DISA-PAC	FBI, NCIS, NSA, NRO	SANS, Carnegie Mellon, Symantec, McAfee	DoD-CERT, Regional CERTS, Component CERTS/CIRTS
DISA	DISA-SCOTT- RCERT	NIPC, USJFCOM, USCENTCOM, USSOCOM, USSOUTHCOM, USSTRATCOM, USTRANSCOM, PAC-CERT, EUR-CERT, COL- CERT, CENT-CERT	CERT/CC, SYMANTEC, MACAFEE, SANS, ARIN, RIPE, APNIC	JTF-CND, DOD-CERT, GNOSC FSO
DSS	n/a	See faxed document, "All Agencies with DCII Over Access". Ask W. Lozano to fax it organizations. (lozanw@saic.com)	Industrial	Air Force, Army, Navy, Marines, DoD agencies (C3, Policy, Comptroller, General Counsel, Washington HQ Services), DLA, DSW, DISA VA, GSAFEDSIM, OPM, State Department, FBI, CIA, NSA, INS, etc.

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
EUCOM	n/a	NATO, NSA, State Department	BAH, PRC, ManTech, Motorola, GTE	IATAC, DISA, NSA
Joint Staff	J6K	most of this survey not applicable because the joint staff - J6 does not do some of the items listed above. We interface with nearly all IA orgs within the govt	msoft and most IA vendors	Services, CINCs, Agencies,
Lincoln Labs	n/a	DARPA, AF (AFRL, AF/ESC, AFIWC, Army (Cecom), NSA, FAA, NIST	BBN, Boeing, Telecordia, SRI, SEI/CERT, Sandia RST, Honeywell, SAIC	
Marines	n/a	FBI, NIPC, NSA, CIA, DIA, DISA, NIST, IOTC, JOIC	Carnegie Mellon University, ISS, Symantec, Macafee, ICSA, CIS, ISSA, IACSS, NCSA, MICROSOFT, Timestep, Dell, Compaq, IBM,	ITFF, AFCEA, ISC2, ISO, IEEE, ANSI, USENET
Navy	NCTAMS	SPAWAR SAN DIEGO, SPAWARSYSCEN CHARLESTON SC, COMNAVCOMTELCOM WASH DC, EUCOM, DISA EUR, NATO, JTF, CNE	SAIC, BBN, CISCO, CABLETRON, DELL CORP, GATEWAY CORP.	SPAWAR SAN DIEGO, SPAWARSYSCEN CHARLESTON SC, SAIC, BBN, DISE EUR
Navy	NCTAMS LANT	CINCLANTFLT AFLOAT AND ASHORE COMMANDS, SPAWAR, CNO, CNCTC, NCTF- CND, FIWC, DCMS, COMNAVBASE, NAVY MID-ATLANTIC REGIONAL COMMANDER, NAVMETOC, JOINT BATTLE CENTER/JTASC, JFCOM, PSD, BUPERS, FISC, CNET, COMNAVTRAGRU, NCIS, DSS, DISA	BOOZ-ALLEN-HAMILTON, SAIC, TDS, LUCENT	CNO, FIWC, SPAWAR, CINCLANTFLT, CNET, NCTF-CND, NCTC, NCIS, DSS, DISA
Navy	NCTAMS PAC	DON CIO ; Chief of Naval Operations (CNO); BUPERS; Flt CINCs; Navy Component Task Force-Computer Network Defense (NCTF- CND); Fleet Information Warfare Center (FIWC); Naval Space Command; Space & Naval Warfare Systems Command (SPAWAR); NAV COMPT; NCT		CNO FIWC, NCTF-CND, SPAWAR, NCTAMS EURCENT, NCTAMS LANT, and NCTAMS PAC

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
Navy	SAF/IG	Defense Criminal Investigative Organizations, Defense Computer Investigations Training Program, DCFL, FBI, NSA, CIA, USSS, DOE, NIPC, JTF-CND, State and Local Law Enforcement, US Dept. of Justice, Various International Law Enforcement Agencies.	Numerous/varied - depending upon investigative requirements	See 10A
Navy	NAVIG			
Navy	NCTAMS PAC	OSD C3I, JS J39/J6, MCEB, IAP, DIAP, JTF- CND, NCTF-CND, DODCERT, service CERTs, NCIS, CINCSPACE, IC CMS, NSA		Same as 'a'
Navy	DONCIO	Federal CIO Council, Federal PKI Steering Committee, NIST, NSA, GSA, GAO, DoD CIO Executive Board, DISA, DLA, DFAS, JECPO, DoD Access Card Office, Other Military Departments, OSD, Joint Staff, OMB, NIPC, US SPACECOM, Treasury, State	Banking Information Technology Secretariat (BITS), RSA, AFCEA	OSD, NSA, FFRDCs, Industry Academia, Joint PMEs, Sandia Laboratories, Gartner Group et al.
NSA	IOTC	National Intelligence Agencies (NSA, CIA, DIA, NIMA, DISA, etc.), Unified Commands, Services (Army, Navy, Air Force, Marine Corps), OSD, DCI.	No direct interface with external industry organizations.	National Intelligence Agencies (NSA, CIA, DIA, NIMA, DISA, etc.), Unified Commands, Services (Army, Navy, Air Force, Marine Corps), OSD, DCI.
NSA	NSA-ISSO	JTF-CND, SPACECOM, NIPC, Other CINCs, Service Certs, NSTISSC members GSA, DTRA, OSD, DISA, NRO	Mitre, CMU-SEI, Cert-CC, SANS and support contractors	NSTISSC members, NIPC, JTF_CND, Service CERTS, etc
OSD	OSD/BMDO	None	None	DoD WHS, C3I ITD
SOCOM	SOCOM-J6	JTF-CND, DISA GNOSC, DoD CERT, Scott RNO SC, other C/S/As, NIPC, NSA, DIA, DISA, JIOC, US Army CECOM, SPAWAR,	Carnegie-Mellon CERT, SANS, CSI,	JTF-CND, USSPACECOM, DISA, NSA,
SOCOM	Army Special Operations Command	ANSOC, ACERT, HQDA, AFSOC, NAVSOC, JSOC, USSOCOM, NSA, NAVCIRT,		Listed in Item A

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
SPACECOM	SPACECOM-J2	USCINCPAC NORFOLK VA/J2//, USCINCPAC HONOLULU HI/J2//, USCINCSOC MACDILL AFB FL/J2//, USCINCEUR VAIHINGEN GE//ECJ2//, USCINCTrans SCOTT AFB IL/J2//, USCINCCSTAT OFFUTT AFB NE/J2//, USCINCCENT MACDILL AFB FL/CCJ2//, USCINCSO MIAMI FL/DRJ2//, USCIN		same as 10(a).
STRATCOM	STRATCOM-J3	DISA, NSA, DIA, CERTs, JTF-CND, CINCs, JIOC, AFIWC, IOTC, Services	Various SW vendors: Symantec, Norton, & Microsoft	DISA, NSA, DIA, CERTs, JTF-CND, CINCs, JIOC, AFIWC, IOTC, Services

APPENDIX E. DIAP PROGRAM DEVELOPMENT AND INTEGRATION TEAM (PDIT) BRIEFING



Defense-wide Information Assurance Program (DIAP) Program Development and Integration

July 2000

David Wilcox
DIAP
703.604.0500
david.wilcox@osd.pentagon.mil

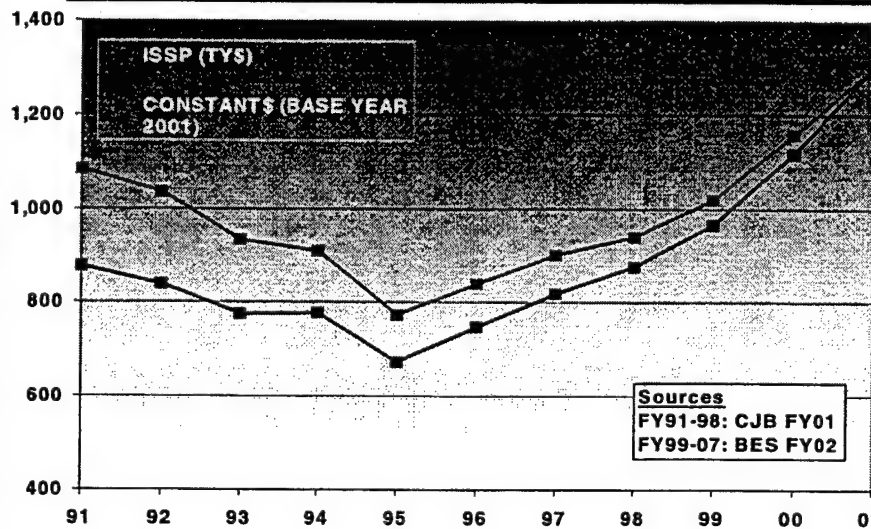


- How much is the DoD spending on IA?
- How much does a pound of IA cost?
- What is the real IA requirement?



What We Know (\$M)

HISTORICAL TREND OF ISSP RESOURCES





What We Don't Know



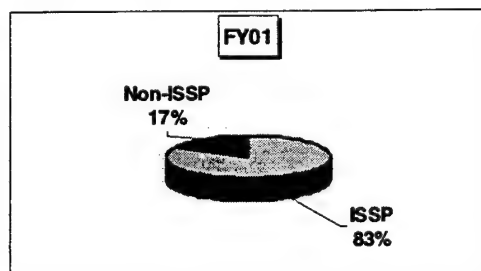
- IA costs embedded within acquisition programs/initiatives
- IC Community
- Services use post, camp, station/base operating support funds for IA
- DOD law enforcement (computer crimes, computer forensic lab)



What We Know (\$M)



Program	FY99	FY00	FY01
ISSP	966.0	1,115.9	1,299.5
Non-ISSP	113.6	185.9	269.5
TOTAL	1,079.6	1,301.8	1,569.0

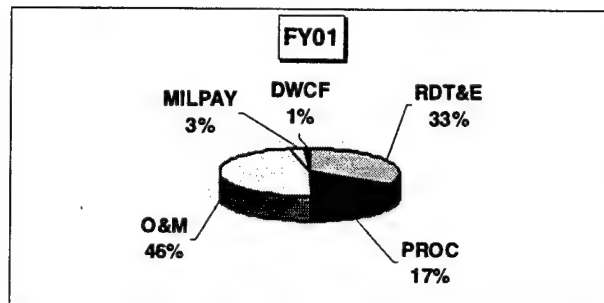




What We Know (\$M)*



Appropriation Cat	FY99	FY00	FY01
RDT&E	392.4	405.0	517.7
PROC	178.1	226.3	263.7
O&M	462.8	611.6	725.2
MILPAY	42.6	44.7	45.8
DWCF	3.7	14.1	16.0
Surcharge	0.0	0.1	0.6
TOTAL	1,079.6	1,301.8	1,569.0



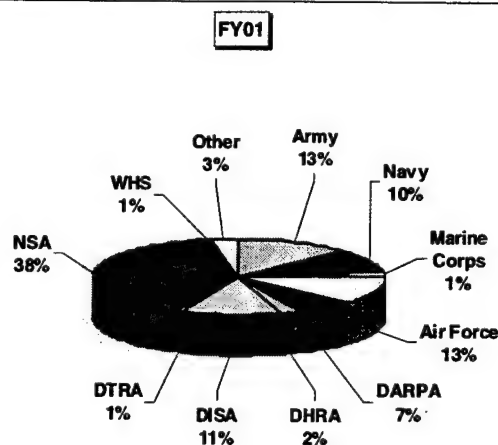
* Does not include Intel IA funding



What We Know (\$M)



Component	FY99	FY00	FY01
Army	113.4	142.0	196.2
Navy	93.7	140.2	161.4
Marine Corps		12.3	20.3
Air Force	116.8	134.3	196.5
BMDO		0.8	1.1
DARPA	77.7	97.5	105.5
DCAA		0.0	0.0
DCMA	2.1	4.1	4.0
DeCA		0.7	1.3
DFAS	1.3	2.5	5.0
DHP	1.7	4.8	6.4
DHRA		13.0	31.8
DIA	0.4	0.4	0.4
DISA	105.0	134.7	173.3
DLA	1.9	7.1	6.8
DSS	0.1	1.1	1.2
DTRA	4.0	6.3	9.4
NMA		0.9	3.0
NSA	545.0	570.5	607.8
OG	0.8	3.0	4.9
OSD	4.2	3.2	3.1
USSOCOM	2.0	2.9	6.6
USTC	0.4	2.7	2.3
WHS	9.4	16.7	20.8
TOTAL	1,079.6	1,301.8	1,569.0

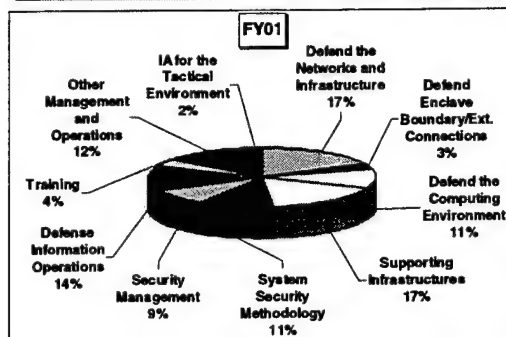




What We Know (\$M)



Defense-in-Depth Category	FY99	FY00	FY01
Defend the Networks and Infrastructure	282.3	238.8	282.6
Defend Enclave Boundary/External Connections	32.4	51.3	39.6
Defend the Computing Environment	64.4	135.4	168.9
Supporting Infrastructures	145.2	184.7	258.1
System Security Methodology	135.0	163.1	168.5
Security Management	96.1	118.3	137.7
Defense Information Operations	121.1	152.7	215.4
Training	41.4	49.7	64.0
Other Management and Operations	154.1	185.7	191.6
IA for the Tactical Environment	7.7	22.2	32.5
TOTAL	1,079.8	1,301.8	1,589.0



Industry IA Estimate



• 5% to 8% * of industry Information Technology spending should be Information Assurance.

- This observation is for network centric IT and does not take into account systems such as the DoD's Strategic and Tactical Weapons/Space Systems (i.e. GPS, NC2, NMD) nor IA Research and Development

• Applied to the DoD

- \$267B Total DoD
- \$ 15.8B DoD IT - (Avg. FY02-07)
- 5-8% = \$.8 - 1.3B

* Source(s) Gartner Group, others



1997 DSB IW-D Recommendation 6.1



- Designate ASD(C3I) as the accountable focal point for all IW issues.
- Establish DASD(IW)

FY99	FY00	FY01
+5	+5	+5

July 2000 Update

OASD(C3I) Information Operations Strategy & Integration chartered as DoD focal point for IO

OASD(C3I)(I&IA) and DIAP Office focal point for IA

FY99	FY00	FY01
+1.5	+2.5	+2.6

For intel-related IA

FY99	FY00	FY01
unable to obtain associated resources		



1997 DSB IW-D Recommendation 6.2



- **6.2.1** SECDEF request DCI to establish a Center for Intelligence Indications & Warning, Current intelligence, and Threat Assessment at NSA with CIA and DIA support

FY99	FY00	FY01
+60	+35	+30

July 2000 Update

NSA's National Security Incident Response Center

FY99	FY00	FY01
2	2	2

Intelligence Resources

FY99	FY00	FY01
unable to obtain associated resources		



1997 DSB IW-D Recommendations 6.2.2 & 6.



- **6.2.2 Establish a Center for IW-D Operations**

FY99	FY00	FY01
+60	+60	+60

- **6.2.3 Establish a Center for IW-D Planning and Coordination**

FY99	FY00	FY01
+10	+10	+10

July 2000 Update

JTF CND / DISA GNOSC / DoD CERT

FY99	FY00	FY01
9.8	12.1	22.0

USCINCSpace assumed CND role for DoD in Oct 1999

FY99	FY00	FY01
-	3.9	14.5



1997 DSB IW-D Recommendation 6.2.4



- **6.2.4 Establish a Joint Office for System, Network, and Infrastructure Design within DISA**

FY99	FY00	FY01
+55	+50	+50

July 2000 Update

OASD(C3I) Architecture & Interoperability Directorate established in 2000

FY99	FY00	FY01
-	~3.0	~3.1

DISA D6 Engineering & Interoperability/Joint Information Engineering Organization (JIEO)

FY99	FY00	FY01
unable to obtain associated resources		

NSA Information Assurance Technical Forum

FY99	FY00	FY01
5	3	3



1997 DSB IW-D
Recommendation 6.2.4
(cont'd)



- **6.2.4 Establish a Joint Office for System, Network, and Infrastructure Design within DISA**

FY99	FY00	FY01
------	------	------

+55	+50	+50
-----	-----	-----

July 2000 Update

Joint IA Architecture Working Group -- IA Info Exchange Requirements

FY99	FY00	FY01
------	------	------

-	<1.0	<1.0
---	------	------

DARPA Info Assurance and Survivability R&D Project

- Research efforts include fault tolerant and survivable network architecture development (see Recommendation 6.9 for DARPA resources)



1997 DSB IW-D
Recommendation 6.3



- **Increase Awareness**
 - Establish IW-D awareness campaign for public, industry, CINCs, Services, Agencies
 - Expand IW Net Assessment in 1994 Summer Study
 - Review Joint Doctrine for IW-D Emphasis
 - Large scale IW-D demos, understand cascading effects
 - Develop simulations to demonstrate IW-D effects
 - Implement Policy to include IW-D realism in exercises

FY99	FY00	FY01
------	------	------

+85	+135	+135
-----	------	------

July 2000 Update

See next 3 slides for update



1997 DSB IW-D
Recommendation 6.3
(cont'd)



- **Increase Awareness**

- Establish IW-D awareness campaign for public, industry, CINCs, Services, Agencies

July 2000 Update

IA awareness raised to highest levels throughout DoD

- DepSecDef strong IA proponent
- OASD(C3I)(I&IA) and DIAP active advocates of IA
- Eligible Receiver 97 demonstrated IA impact on operations
- Continuous series of attacks/probes on DoD networks
- USSPACECOM assigned CND/CNA operational mission
- Quality and degree of DoD IA Training/awareness significantly raised
- DoD and Services have "IA Awareness" days and conferences
- Awareness processes exist that engage with industry and academia

FY99	FY00	FY01
14	16	19



1997 DSB IW-D
Recommendation 6.3
(cont'd)



- **Increase Awareness**

- Expand IW Net Assessment in 1994 Summer Study
- Review Joint Doctrine for IW-D Emphasis
- Large scale IW-D demos, understand cascading effects

July 2000 Update

Status and efforts to expand 1994 IW Net Assessment are unknown

OASD(C3I)(Info Ops Strategy & Integration)

- Conducting IO Broad Area Review with DoD Components, including IA
- Services and JS, in conjunction with IO review, are reviewing IO and IA doctrine

Joint Warrior Interoperability Demonstration (JWID)

- Ongoing right now, some IA technologies to be demonstrated



1997 DSB IW-D
Recommendation 6.3
(cont'd)



- **Increase Awareness**
 - Develop simulations to demonstrate IW-D effects
 - Implement Policy to include IW-D realism in exercises

July 2000 Update

Components have some modeling and simulation efforts to demonstrate IA effects and to collect data. Most of these efforts reside at NSA

JS is staffing CJCSI 6510.01 to:

- include integration of CND (IA) into joint exercises and wargames
- instruct components to exercise CND in realistic scenarios
- task J7 to ensure IA and CND operations are exercised and coordinated

Components are implementing IA (to varying degrees) into exercises

- INFOCON 99, Blue Flag 00-2, 00-3, UFL, Steel Puma, Power Sweep...



1997 DSB IW-D
Recommendation 6.4



- **Assess Infrastructure Dependencies and Vulnerabilities**

prior FY99 FY99 FY00 FY01

+90 +0 +0 +0

July 2000 Update

DoD Critical Infrastructure Protection (CIP)

CIP Office with staff of nine

FY99	FY00	FY01
<1	<1	<1

CIP Analysis and Assessments

Joint Program Office Special Technologies Countermeasure (Navy)

FY99	FY00	FY01
14	14	14

Balanced Survivability Assessments (DTRA)

FY99	FY00	FY01
-	-	10

ASD(C3I) Y2K/CIP

FY99	FY00	FY01
20	-	-



1997 DSB IW-D
Recommendation 6.5



• **Define Threat Conditions and Responses**

FY99 FY00 FY01

+0 +0 +0

July 2000 Update

INFOCONS

- VJCS signed memo March 10, 1999 on INFOCON procedures and policy
- JS revising CJCSM 6510.01 to include INFOCON, hopefully this Fall



1997 DSB IW-D
Recommendation 6.6



• **Assess IW-D Readiness**

- Establish standardized readiness assessment system
- Incorporate IW preparedness assessments in Joint Reporting systems and Joint Doctrine

FY99 FY00 FY01

July 2000 Update

CJCSI 6510.04 IA Readiness Metrics issued May 15, 2000

- Provides standardized IA metrics and supplemental policy IA guidance to support DoD components self-assessment of IA status for consideration in Joint Monthly Readiness Report (JMRRs)
- Future guidance/policy on incorporation into SORTS type reports is under consideration



1997 DSB IW-D Recommendation 6.7



- "Raise the Bar" with high-payoff, low-cost items
 - Improve access control (get rid of fixed passwords)
 - Identification and authentication
 - Examine products, use approved products

FY99	FY00	FY01
+10	+10	+10

July 2000 Update

DoD Public Key Infrastructure program (managed by NSA)

FY99	FY00	FY01
20	56	127

Enabling of applications to utilize a public key infrastructure

- PKE to be resourced from components' programs
- PKE study estimates total resources to PK-Enable 690 applications will be around \$175M

National Information Assurance Partnership (NIAP)

FY99	FY00	FY01
3	7	4



1997 DSB IW-D Recommendation 6.8



- Establish and maintain a minimum essential information infrastructure
 - Define options with associated costs and schedules to determine MEII such that infrastructures can failsoft to support critical functions while under attack
 - Define minimum essential conventional *force structure* and supporting *information infrastructure* needs
 - Prioritize critical functions and infrastructure dependencies
 - Design a Defense MEII and a failsafe restoration capability
 - Direct Components to fence funds for Defense MEII and restoration capability

FY99	FY00	FY01
+100	+100	+100

July 2000 Update

Separate & limited efforts ongoing to define MEII.

- CIP office analyzes defense sectors and identify MEIIs, but not all.
- OASD(C3I) is working to define supporting info infrastructure.
- The National Security Telecommunications Advisory Committee (NSTAC) coordinates with industry to assess telecommunications interdependencies for Governmental critical mission operations and may address MEIIs.



1997 DSB IW-D
Recommendation 6.9



- **Focus the R&D on following areas:**
 - Robust survivable system architectures
 - Techniques and tools to model large scale distributed network systems
 - Tools for synthesizing & projecting performance of survivable distributed systems
 - Testbeds and simulation-based mechanisms for evaluation of emerging technologies
 - Research in US Computer science and engineering programs
 - Educational programs for curriculum development at undergrad and graduate levels

FY99	FY00	FY01
+125	+160	+160

July 2000 Update

See next slide for update



1997 DSB IW-D
Recommendation 6.9
(cont'd)



- **Focus the R&D effort**

FY99	FY00	FY01
+125	+160	+160

July 2000 Update

NSA IA Research and Development

FY99	FY00	FY01
49	57	60

DARPA Info Assurance and Survivability R&D Project

FY99	FY00	FY01
78	99	115



1997 DSB IW-D **Recommendation 6.10**



- **Staff for Success**
 - Establish career paths, training & certification of systems administrators
 - Establish a skill specialty for IW-D
 - Develop specific IW awareness courses with focus on DoD's professional schools

FY99	FY00	FY01
------	------	------

+55	+50	+50
-----	-----	-----

July 2000 Update

IA mobile training teams

DoD wide training and certification of military, civilian, and contractor:

- IS Administrator/Security Manager/Security Officer
- IS Professional technician

FY99	FY00	FY01
------	------	------

18	24	26
----	----	----

IA & IT Training, Certification, and Personnel Management Report

- With DEPSECDEF for review and signature
- Estimates \$77.5M over FYDP to implement all recommendations



What We Should Know



- DOD's total IA resources
- What it buys us
 - Risk return on investment
- What is the total requirement

APPENDIX F. ACRONYMS

AFIWC	Air Force Information Warfare Command
BIOSG	Bilateral IO Steering Group
CERTs/CIRTs	Computer Emergency or Incident Response Teams
CIP	Critical Infrastructure Protection
CJCS	Chairman of Joint Chiefs of Staff
CNA	Computer Network Attack
CND	Computer Network Defense
COMSEC	Communications Security
CONOPS	Concepts of Operations
COOP	Continuity of Operations Plan
COP	Common Operational Picture
CORT	Cyber Operations Readiness Triad
DepSecDef	Deputy Secretary of Defense
DIAP	Defense-wide Information Assurance Program
DIO	Defensive Information Operations
DoD	Department of Defense
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
ETA	Education Training and Awareness
ETS	Education and Training for Service
FEA	Front End Assessments
FIWC	Fleet Information Warfare Command

FOC	Full Operational Capability
GAO	Government Accounting Office
GCCS	Global Command and Control System's
GIG	Global Information Grid
GNOSC	Global Network Operations and Security Center
IA	Information Assurance
G&PM	Guidance & Policy Memo
IA/IT HR IPT	Information Assurance/Information Technology Human Resources Integrated Process Team
IC	Intelligence Community
IDM	Information Dissemination Management
IO/IA/CIP	Information Operations, Information Assurance, and Critical Infrastructure Protection
IPT	Integrated Process Team
ISSP	Information Systems Security Program
I&W	Indications and Warning
JMRR	Joint Mission Readiness Review
JPO-STC	Joint Program Office for Special Technology Countermeasures
JRDC	Joint Requirements Oversight Council
JTF-CND	Joint Task Force-Computer Network Defense
JTS	Joint Training System
MCB	Marine Corps Base
NETOPS	Network Operations
NOIWON	National Operations and Intelligence Watch Officer Network

NORAD	North American Air (later) Aerospace Defense Command
NSTISSC	National Security Telecommunications and Information Systems Security Committee
OMB	Office of Management & Budget
OPM	Office of Personnel Management
ORA	Operational Readiness Assessment
OT&E	Operational Test and Evaluation
PA&E	Program Analysis and Evaluation
PE	Program Element
PPBS	Planning Program and Budgeting System
PRG	Program Reviews
RC	Reserve Component
RDT&E	Research Development Test and Evaluation
ROE	Rules of Engagement
R&D	Research & Development
SecDef/OSD	Secretary of Defense/Office of the Secretary of Defense
SBU	Sensitive-but-Unclassified
SOP's	Standard Operating Procedures
TCCC	Theater C4 Coordination Center
TPI	Two-person Integrity
TTP	Tools, Tactics, Techniques, Procedures
USCINCSpace	Commander in Chief, U.S. Space Command
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology & Logistics

USD(P)	Under Secretary of Defense Policy
USMC	United States Marine Corps
VA	Vulnerability Assessment
VE	Vulnerability Evaluation
WMD	Weapons of Mass Destruction

ANNEX D

Defense Science Board Task Force on Defensive Information Operations

Panel Report on Policy Implications

REPORT OF FINDINGS, DISCUSSION/OBSERVATIONS AND RECOMMENDATIONS

TABLE OF CONTENTS

Executive Summary	1
1. Low Entry Cost	2
2. Blurred Traditional Boundaries.....	2
3. Expanded Role For Perception Management.....	2
4. Lack Of Strategic Intelligence.....	3
5. Difficulty Of Tactical Warning And Attack Assessment.....	3
6. Difficulty In Building And Sustaining Coalitions.....	3
7. Vulnerability of the United States Homeland	3
Conclusions	6
I. Toward a Common Terminology.....	7
Findings.....	7
II. Requirement for Government-Wide Coordination	9
Findings.....	11
III. Critical Infrastructure Protection.....	13
Findings.....	15
VI. Security Standards.....	17
Findings.....	19
Appendix A. Acronyms.....	21
Annex B. Panel Membership	23

EXECUTIVE SUMMARY

"We can't solve problems by using the same kind of thinking we used when we created them."

Albert Einstein

The American homeland is becoming increasingly vulnerable to non-traditional attack, including information warfare, the focus of this report. Rapid advances in technology have and will continue to create new vulnerabilities and challenges to U.S. security. Recent studies by both the Government Accounting Office (GAO) and the Computer Security Institute found that the number of cyber security threats to both the government and the private sector is on the rise. The damage caused by a successful attack, both to physical infrastructures and to the psychological health of U.S. institutions, could prove immense, and the Department of Defense is not exempt from this danger.

In many circles within the U.S. defense and broader international security community, the term "information warfare" is increasingly being used to encompass a far greater set of information-age "warfare" concepts than was attributed to it in the past. These emerging new warfare concepts are directly tied to the prospect that the ongoing rapid evolution of cyberspace, the global information infrastructure, could bring both new opportunities and new vulnerabilities. At least one of these vulnerabilities, the prospect that the information revolution could put at risk high-value national assets outside the traditional battlespace boundaries, will affect U.S. national security strategy, and thus U.S. military strategy. The fact that assets that are critical to the conduct of military operations would also be put at risk compounds this problem.

There is an emerging element of information warfare, one that appears to be common to almost all currently evolving uses of the term, which warrants identification and definition. Strategic information warfare, in essence, the intersection of evolving information warfare and post-cold war "strategic warfare" concepts, warrants special recognition and attention as a legitimate new facet of warfare, one with profound implications for both U.S. military strategy as well as overall U.S. national security strategy and policy.

A fundamental aspect of strategic information warfare is that *there is no front line*. Strategic targets in the United States may be just as vulnerable to attack as in-theater command, control, communications, and intelligence targets. As a result, there exists a need for broadening strategic understanding beyond the single traditional regional theater of operations to four distinct separate theaters of operation: 1) the battlefield, 2) the allied or regional zone of the interior, 3) the intercontinental zone of communication and deployment, and 4) the U.S. zone of the interior.

The post-cold war "*over there*" focus contained in the persistent emphasis on the regional component of U.S. military strategy has been rendered incomplete and is of declining relevance to the likely future international strategic environment. When responding to information warfare attacks of this character, military strategy can no longer afford to focus on conducting and supporting operations only in a region of concern.

What are the basic features of strategic information warfare as best we understand them today? The following represent a synthesis of observations about these basic features. There is, most definitely, a cascading effect inherent in these observations; each helps to create the enabling conditions for subsequent ones.

1. LOW ENTRY COST

Interconnected networks may be subject to attack and disruption not just by states but also by non-state actors, including dispersed groups and even individuals due to the low cost of entry. Potential adversaries could also possess a wide range of capabilities. Thus, the threat to U.S. interests could be multiplied substantially and will continue to change as ever more complex systems are developed and requisite expertise is ever more widely diffused.

Cyber attacks have moved beyond the realm of the mischievous teenager and are now being learned and used by terrorist organizations as the latest weapon in a nation's arsenal. In June 1998 and February 1999, the Director of the Central Intelligence Agency testified before Congress that several terrorist organizations believed information warfare to be a low-cost opportunity to support their causes. Both *Presidential Decision Directive 63* (PDD-63) issued in May 1998 and the *President's National Plan for Information Systems Protection*, version 1.0, issued in January 2000, call on the legislative branch to build the necessary framework to encourage information sharing to address cyber security threats to our nation's privately held critical infrastructure.¹

Effective attribution and swift response to attacks would nullify the appeal of the low cost of entry by making the chances of "getting caught" much higher. Perceived increased risk by the attacker should be an added deterrent to preventing information warfare attacks.

2. BLURRED TRADITIONAL BOUNDARIES

Given the wide array of possible opponents, weapons, and strategies, it becomes increasingly difficult to distinguish between foreign and domestic sources of information warfare threats and actions. We may not know who is under attack by whom, or who is in charge of the attack. This greatly complicates the traditional role distinction between domestic law enforcement, on the one hand, and national security and intelligence entities on the other.

Not only are borders becoming more porous, but they are increasingly irrelevant in cyberspace. According to a long-time CIA operative and FBI consultant, "Globalization and technology were lowering traditional boundaries between what constitutes an international or domestic threat, and terrorists, drug cartels, spies, and hackers were all leaping those boundaries with impunity."²

3. EXPANDED ROLE FOR PERCEPTION MANAGEMENT

Opportunities for information warfare agents to manipulate information that is essential to public perceptions may increase. For example, political action groups and other non-government organizations can use the Internet to galvanize political support, as the Zapatistas in Chiapas,

¹ Statement of Representative Tom Davis on the Introduction of The Cyber Security Information Act of 2000, April 12, 2000.

² John McGaffin, in *Covert Counterattack*, by James Kitfield, National Journal, September 16, 2000, pg. 2858.

Mexico, were able to do. Furthermore, the possibility arises that the very "facts" of an event can be manipulated via multimedia techniques and widely disseminated. Conversely, there may be decreased capability to build and maintain domestic support for controversial political actions. One clear implication is that future U.S. administrations may include a robust Internet component as part of any public information campaign.

4. LACK OF STRATEGIC INTELLIGENCE

For a variety of reasons, traditional intelligence-gathering and analysis methods will be of limited use in meeting the strategic information warfare challenge. Collection targets will be difficult to identify using existing national technical means; allocation of intelligence resources will be difficult because of the rapidly changing nature of the threat; and vulnerabilities as well as target sets will not be well understood. In sum, the United States may have great difficulty identifying potential adversaries, their intentions, and their capabilities.

5. DIFFICULTY OF TACTICAL WARNING AND ATTACK ASSESSMENT

Warning and attack characterization and assessment involving information warfare presents fundamentally new problems in a cyberspace environment. A basic problem exists: distinguishing between attacks and other events such as accidents, system failures, or hacking by thrill seekers. This challenge is exacerbated by the speed of events in cyberspace. The main consequence of this feature is that the United States may not know when an attack is underway, who is attacking, or how the attack is being conducted.

6. DIFFICULTY IN BUILDING AND SUSTAINING COALITIONS

Many allies and coalition partners will be vulnerable to information warfare attacks on their core information infrastructures. For example, the dependence on cellular phones in developing countries could well render telephone communications in those nations highly susceptible to disruption or deception. Other sectors in the early stages of exploiting the information revolution, such as the energy or financial sectors, may also present vulnerabilities that an adversary might attack to undermine coalition participation. Such attacks might also serve to sever weak links in the execution of coalition plans.

Conversely, tentative coalition partners who urgently need military assistance may want assurances that a United States deployment plan to their region is not vulnerable to information warfare disruption.

7. VULNERABILITY OF THE UNITED STATES HOMELAND

As stated earlier, information warfare has no front line. Potential battlefields are anywhere networked systems allow access. Current trends suggest that the United States economy will rely on increasingly complex, interconnected network control systems for such necessities as oil and gas distribution management, electric grids, telephone service, air traffic control, and much, much more. The vulnerability of these systems is currently poorly understood. This lack of understanding and recognition inhibits a thorough assessment of the vulnerabilities that may exist in both the technology-driven control systems and in the fiscal marketing processes that can directly affect energy distribution. In addition, the means of deterrence and retaliation are uncertain and may rely on traditional military instruments in addition to information warfare

threats. In summary, the United States homeland may no longer provide a sanctuary from outside attack.

The U.S. concept of national security must adapt to this changing world. The existing national security decision-making and execution apparatus is not well suited to ensure this type of security. Among other things, the apparatus that is needed must be able to:

- Act quickly, avoiding the delays of inter-agency processes, yet represent appropriate concerns
- Deal with threats functionally instead of geographically
- Bring law enforcement, national defense, and intelligence functions to bear on a threat seamlessly without endangering civil liberties
- Engage with the private sector

Rebuilding the national security apparatus cannot be done in one step. The bipartisan Commission on National Security in the 21st Century has begun to address this problem. It must evolve and adapt as the world changes. The key will be to create a flexible, agile, adaptive apparatus that embraces experimentation and keeps what works.

In the interim, this panel submits a series of recommendations, grouped into four areas, the implementation of which would go a long way to meet the emerging information warfare threat. The panel believes that actions taken in the near term would materially benefit the effective execution of Defensive Information Operations (DIO) within the Department.

RECOMMENDATION 1

Create an Executive Order (EO) on Common DIO Terminology

Multiple definitions for the same DIO-related terms are in wide usage within DoD, DOJ, and the Intelligence Community (IC). The absence of common definitions produces differing interpretations of authorities and knee-jerk reactions in both the private sector and the legal community, e.g., monitoring, attack, armed attack, etc. This decreases the likelihood of coordination and increases the potential for confusion and turf battles. We believe the problem can be solved by using existing mechanisms without changing current laws, policies; and regulations. The recently signed Presidential Review Directive (PRD) will institute an Interagency Working Group (IWG) process that will help.

The SecDef and the Director of the Critical Infrastructure Assurance Office (CIAO) should jointly sponsor an effort to produce an authoritative document (perhaps an EO) containing the maximum number of DIO-related terms, which would be useful to Information Assurance (IA) in a national, DoD, civil agency, and civil context.

RECOMMENDATION 2

Establish a National DIO Coordinator

The nation has no means of providing either tactical Indications and Warning (I&W) of a widespread cyber attack on critical infrastructures or a coordinated response to it. No one is assigned the clear responsibility for rationalizing law enforcement and national defense equities when a cyber attack is detected. There is currently a bias in favor of law enforcement procedures, even if their use impedes response and recovery. There is no governing authority with the responsibility to make response-and-recovery decisions effective across stovepipes. Moreover, coordination often depends on the personalities of those involved.

The SecDef should propose creation of a national DIO coordinator. Initial responsibilities and authorities would be limited to policy and planning, but would increase as the job matures and Congress engages, to potentially include: oversight, direction and control, responsibility for information resource policy and strategic planning and adjudication among agencies.

RECOMMENDATION 3

Identify Critical Infrastructure Dependencies

Critical infrastructures are those systems that are essential to the minimum operations of the economy and government. The critical infrastructures of the United States are predominantly owned by the private sector, and the DoD is extremely dependent upon them. Industry has indicated a willingness to share information with the DoD, but will not necessarily be motivated by the same factors that motivate government. Industry fears regulation and unfunded mandates and will not go beyond what makes financial sense.

DoD must make a concerted effort to identify what is critical in terms of its private sector infrastructure dependencies. The DoD effort to produce sector Critical Infrastructure Protection (CIP) plans was a step in the right direction; however, lack of funding is hindering this action. DoD must energize its local outreach by local DoD installation commanders to build the relationships necessary and to identify dependencies on local commercial and municipal infrastructures.

RECOMMENDATION 4

Gain Consensus on DIO Security Standards

There are few information security technical standards to which DoD program managers can turn. Moreover, Global Information Grid (GIG) Information Assurance Technical Architecture Framework (IATF) Standards and Protocols for providing security are inconsistent with the Joint Technical Architecture (JTA).

A clarification memorandum should be issued making it clear the JTA will be adhered to for all GIG implementations, especially in the IA domain. The JTA is the better reference on IA standards and protocols, and it should be referenced as such in all GIG IA policy documents.

CONCLUSIONS

Following the end of the Cold War, and the subsequent changes in the geopolitical climate, the United States now faces a different kind of threat. This threat is characterized by the ability of numerous potential adversaries to engage in an information attack upon the United States, enabled by the lower entry costs associated with such an attack. Further, an attack could be at a lower threshold as a concerted effort to undermine or gradually erode our strategic or tactical position, our economic strength and fiscal processes, societal confidence in our government's ability to respond to crisis, or other less traditional targets. America's ability to attribute and respond is woefully insufficient to pose a significant deterrent to would-be attackers. And on the other end of the spectrum, early tactical indications and warning capabilities are virtually non-existent in cyberspace. These factors converge to create a newly and differently vulnerable United States homeland.

It is our contention that immediate actions can work to decrease the threat and potential damage to United States national security, including infrastructures, institutions, and individuals. The United States national security apparatus must continue to evolve over time to deal with these emerging trans-national threats, including trans-boundary threats where the differences between law enforcement and national defense, between foreign and domestic, between national and transnational, and between government and civilian are increasingly irrelevant. In the interim, there are a few discrete policy related actions we as a nation and military institution should take:

- We all need to be able to speak the same language and should take action toward a common DIO-related lexicon.
- Someone needs to be in charge to ensure government-wide coordination.
- We need to identify our dependencies on and protect our critical infrastructures.
- DOD systems developers need a single source for DIO security standards.

I. TOWARD A COMMON TERMINOLOGY

New technologies and new concepts inevitably require new terminology. Unfortunately, terminology and definitions related to DIO vary widely throughout government and the private sector. DoD has expended considerable effort to standardize Information Operations (IO) related definitions, but differences and controversy remain. The Intelligence Community (IC) and DoD, in spite of a great incentive to share definitions, have managed to formally agree on only about a dozen. Industry and the private sector use a wide variety of definitions depending on convenience and circumstance, and these often differ from those within the IC and DoD.

How one defines a concept or an action has a direct bearing on which laws may be applicable to a situation and which authorities may hold sway. It may also affect how actions are funded. Consequently, definitional issues often masquerade as surrogates for deeper struggles over turf and resources.

The situation is made more complicated by the fact that some terms arrive on the scene laden with semiotic baggage. For example, "monitoring," means one thing to the National Security Administration (NSA) in a foreign intelligence context, another to the FBI in its law enforcement role, and something quite different to the ACLU when discussing the Fourth Amendment. Likewise, the term "attack" may mean to destroy, to penetrate for purposes of monitoring, to trace back for purposes of defense, or to temporarily disable, depending on who is conducting the "attack" and the intent of his or her actions.

Fortunately, the law does not need to be changed to create a common lexicon and direct its use throughout government. Most, if not all, of the problems associated with definitions can be solved using existing processes and organizations. However, a necessary precondition of such a lexicon would be an improved consensus on authorities, roles, and responsibilities to perform DIO. The process of building a common lexicon would force many such issues into the open for discussion and resolution. Additionally, if such a lexicon were developed with utility to the civil sector in mind, it might have the added benefit of helping industry consolidate its efforts to defend critical infrastructures.

A Presidential Review Directive (PRD) has recently been signed, which calls for an Interagency Working Group (IWG) to reach consensus on several matters important to IO in general and DIO in particular. Doing so will do much to clarify roles and responsibilities. The subject of definitions is among the matters to be discussed, but the PRD stops short of calling for a comprehensive common lexicon to be used throughout government.

FINDINGS

- Multiple definitions exist for common DIO-related terms. This is so within both DoD and the IC. The law enforcement community, the private sector, and the rest of government use either their own terms for DIO-related concepts or create new ones as the need arises.
- Within DoD and the IC, the use of multiple definitions for the same concept has the potential to cause operational confusion. Outside of DoD and the IC, the use of

multiple terms can exacerbate problems associated with overlapping authorities and complicate efforts to coordinate a response to an attack.

- The absence of common definitions produces differing interpretations of authorities and differing ideas about the purpose of an action. This can be particularly troublesome when particular words (e.g., monitoring) have widely accepted meanings in the private sector and legal communities, which are based on case law or popular misconceptions.
- A common lexicon would not only facilitate mutual efforts to defend infrastructures, but it would help clarify authorities, roles, and responsibilities as well.
- Creating a common lexicon of useful DIO terms would not require changes to law, policy or regulation. Existing mechanisms and organizations are sufficient to mandate and develop such a lexicon.
- The challenge will be to reach out beyond DoD and the IC to include the private sector, the law enforcement community, and the rest of government in the process. For this reason, the effort requires sponsorship at the National Security Council (NSC), National Economic Council (NEC), or Executive Office of the President (EOP) level.

RECOMMENDATIONS

- SecDef and the Director of the CIAO should jointly sponsor an effort to produce an authoritative document (perhaps an Executive Order) containing DIO-related terms, which would be useful in both the national security and civil sectors of government. This effort should draw upon the work of the IWG established by the PRD on IO.
- To assist this effort, the following Office of the Secretary of Defense (OSD) actions should be undertaken:
 - DOD & IC General Counsels (GCs) should work with the DOJ to develop a common concept for and set of terms to be used when conducting “investigations” in cyberspace.
 - The Bilateral IO Steering Group (BIOSG) should create a joint DOD/IC working group to produce the largest possible set of common IO-related definitions. The term DIO should be included.
 - USD(P) should initiate a dialogue with the State Department and the Office of Management and Budget (OMB) regarding common DIO definitions. The goal of these talks would be to encourage the use of common DIO-related terms throughout top levels of government, the international community, and the DoD.

II. REQUIREMENT FOR GOVERNMENT-WIDE COORDINATION

Prior to the Information Age, protecting the nation from external attack was clearly the province of the DoD, supported by the IC. Law enforcement assisted with counter-intelligence efforts and other domestic responsibilities. The situation is more complex today. An attacker in cyberspace may do harm to our critical infrastructures without our knowing his identity or location. The infrastructures he is attacking may be private property and not clearly under the purview of the national security apparatus. Similarly, uncertainty about the origin, severity, and target of an attack may lead to confusion over whose authorities are preeminent in responding to it. Obviously, coordination becomes critical in such circumstances.

Warning is another issue that will be seen through different lenses in the Information Age. Traditional intelligence collection and analysis methods might provide some measure of *strategic* warning of an IO attack, but the nation has no means of providing *tactical* Indications and Warning (I&W) in cyberspace. In fact, there is no reliable means of even detecting a widespread, subtle, "slow and low" attack, let alone warning of it. Some would argue that such an attack is already ongoing. Even if an attack were detected, there is no consistent, widely understood process for reacting to it or recovering from its effects. Furthermore, there are no formal mechanisms for balancing equities between law enforcement and national security when reacting to it.

Any cyber I&W effort will require visibility into a large number of domestic networks, if not for content, at least to characterize the health of their operations. Obviously, the IC is limited in its ability to perform such a function. Likewise, law enforcement is proscribed from monitoring actions in the absence of compelling legal grounds. Nevertheless, there is much that can be done within existing law, policy, and regulation. (For a more complete discussion of this subject, see the legal section of the report.)

A few systems in government and industry (e.g., monitored command networks and Telecommunications Service Providers) have limited capabilities to detect an attack within their own "stovepipes," but reaction options are limited and local. Coordination and "spreading the word" generally falls to Computer Emergency Response Teams (CERTs) and individual initiative. In no case is there a robust means of characterizing diverse attacks occurring in separate segments of government and industry or of rationalizing large-scale reaction and recovery. The National Information Protection Center (NIPC) was originally created to help coordinate information on such attacks, but has devolved primarily into a cyber-crime investigation body. In fact, the predominant FBI (law enforcement) culture of the NIPC has made information sharing difficult in a practical sense, within government or with industry. As always, well-meaning individuals with initiative have built informal coordination mechanisms, but these are personality dependent.

Since the NIPC, by default, considers a cyber intrusion to be a crime, rules of evidence and strict investigative procedures are applied and information sharing is restricted. This practice, which appears to have little justification in law, biases reactions in favor of law enforcement and

stands in the way of effective information sharing and the coordination that would be necessary to mount an effective national defense. Finally, no one is assigned the responsibility or the authority (other than through Cabinet level cooperation) to make the decision that an ongoing attack has progressed from a law enforcement case to a national security matter.

A similar vacuum is seen when one looks for someone in authority to coordinate a recovery from a nationwide or large-scale cyber attack. Obviously, some activities would be covered under standing contingency plans for disaster recovery or continuity of government. Likewise, many segments of industry, (e.g., banking and the stock markets) have elaborate backup and recovery plans. On the other hand, if an attacker were to mount a carefully coordinated assault on several segments of our infrastructure simultaneously, it would be difficult to recover without massive dislocation. For example, if phone service and the power grid were lost at the same time gas lines were disrupted during winter, the combined effect could be catastrophic. Even worse would be a scenario combining such cyber attacks with traditional bomb blasts or the release of a biological agent. It does not take much imagination to see that coordinating a recovery would require difficult tradeoff decisions about whose infrastructure should be recovered first. Questions of liability aside, these hard choices must be made by someone with visibility across infrastructure stovepipes and the authority to compel actions that will affect lives and finances.

As matters stand today, a declaration of martial law might be required to answer the demands of the desperate situation described above. However, a more palatable, more effective, and less costly recovery could be made using the offices of a standing official charged with the responsibility for national critical infrastructure protection. It is true that there is a coordinator for counterterrorism, security and critical infrastructure protection, but realistically his authorities are constrained to his powers of persuasion. Likewise, CINC, Joint Forces Command is charged with homeland national defense, but confusion may arise from the fact that CINCSpace is responsible for Computer Network Defense. Realistically, neither CINC can do much to prepare for homeland cyber defense without asking hard questions about posse commitatus, the legal aspects of dealing with private industry, and public perceptions of the military taking on such a role in peacetime.

Finally, there is the question of international allies and corporations with close ties to U.S. firms. Geographic boundaries mean little in cyberspace. Effective reaction to and recovery from a serious cyber attack almost certainly will require coordination with allies and foreign partners. Consequently, the State Department must engage on these issues in the immediate future. In fact, State is already involved in several DIO-related matters, such as a Russian proposal to limit work on Information Warfare. As matters progress, State will have to join more fully with the DoD, the IC, and law enforcement communities in coordinating responses to cyber issues.

In sum, the nation needs a well-staffed, designated official with direct access to the principals of the National Security Council (NSC) who is charged to plan for and respond to the type of crisis described above. Perhaps the growing discussion about creating a Federal CIO within the Executive Office of the President will answer these concerns, provided that the position is given the required authorities and that national security matters are coordinated through the NSC. Such an official will require explicit authorities that can only be granted in law by Congress. Consequently, anyone appointed to fulfill these duties will require Congressional confirmation.

FINDINGS

- We have no means of providing tactical I&W of a widespread, well-coordinated cyber attack, other than reporting within a few stovepipes (e.g., local telcos and DoD networks).
- There is no clear responsibility for rationalizing law enforcement and national defense equities when certain types of cyber attack are detected.
- There is currently a bias toward using law enforcement authorities and procedures when a cyber incident is detected. Although this will be satisfactory in the vast majority of cases, no formal means exists to review cases to determine if national security procedures might be more appropriate.
- No one has the responsibility or authority to make response and recovery decisions and take actions across stovepipes. Coordination depends on personalities.
- The State Department is potentially very important to DIO, but is not sufficiently engaged.
- A great portion of government does not understand DIO issues or appreciate the potential impact of information technology vulnerabilities on their operations.

RECOMMENDATIONS

- The SecDef should propose the creation of a national DIO coordinator. Prior to congressional action, the Coordinator's authorities will be limited. In the interim, he could serve as the nexus of DIO policy development. Eventually, this individual should sponsor the development of national-level, coordinated DoD/IC/law enforcement mechanisms to provide I&W of a cyber attack, respond to it, and recover from its effects.
- To support this effort the SecDef and DCI should:
 - Create a joint DoD/IC panel to work with the DOJ, NSC, and OMB staffs to draft a DIO Executive Order (EO). The EO should clearly establish the preeminence of the national security response over the law enforcement response in cases having a national security impact.
 - Create a panel to examine EO12333 and other law, policy, and regulations in light of emerging DIO realities.
 - Create a standing GC's working group to monitor legal precedents for decisions useful and inimical to DIO efforts and to explore the latitude available for DIO under existing law.
 - Task the Bilateral IO Steering Group (BIOSG) to propose mechanisms for the military services and the IC to deconflict DIO (especially related to Computer Network Operations).

III. CRITICAL INFRASTRUCTURE PROTECTION

The Defense Department is increasingly reliant on a broad range of vital infrastructure services provided by the private sector, municipal utilities, and other non-DoD sources. While DoD's communications, energy, transportation, logistics, and supporting requirements grew significantly over recent decades, DoD has become far more dependent on non-DoD-owned and -operated systems and networks. The underlying private sector infrastructures have undergone an explosion in technical capability, complexity, and integration, adopting new technologies and processes, particularly evident in communications and energy infrastructures. This revolution in technology and system interoperability has empowered infrastructure owners and operators to better serve their customers while expanding capabilities and building corporate strength. Technological interoperability, a feature inherent in these infrastructures, was market economy driven, and thus the infrastructures are exceedingly interdependent. As the infrastructures advanced in capability, capacity, and complexity, DoD took advantage of their availability.

Private sector dependencies have direct implications for the availability and reliability of DoD's Global Information Grid (GIG) – leased private sector systems incorporating our nation's fiber optic network, twisted wire, and wireless systems provide the GIG's backbone outside DoD's information infrastructure gateways. The dependencies go much further than this vital information backbone; the breadth of defense operations requires much more energy, logistics, and other vital services than ever before. For DoD to fully understand its private sector dependencies, it must analyze and assess those dependencies, a process that cannot be done without dialogue and partnering with the private sector or municipal owners and operators of those infrastructures.

DoD's expanded use of private sector infrastructures should logically require a more detailed assessment of potential risks inherent in the interdependent, underlying infrastructure. The private sector built and operated these infrastructures while using a very different risk model than those used within DoD. Private sector risk analyses are based on economically driven models, focusing on profitability and customer service, with modernization reliant on anticipated returns on investment. Threats and risks are plausible in peacetime scenarios, where the threats may be backhoes and risks considered are seen as natural disasters or competitive business practices. DoD risk models focus on more sinister threats – where a bad actor or nation state could purposefully deny infrastructure to degrade our global projection of force or otherwise undermine the national security of the United States.

The *Presidential Decision Directive on Critical Infrastructure Protection* (PDD-63, 1998) focused national efforts to implement critical infrastructure solutions, including expanded partnership between government and the private sector. Many national initiatives began, including establishment of the National Infrastructure Protection Center at FBI and the initiation of Infrastructure Sector Analysis Centers (ISACs), attempting to expand partnership between government and the private sector within individual infrastructure sectors. Arguably, though much has been done to advance national CIP efforts, the broad ranging initiatives have not seemed to gel into the desired partnerships, including interagency coordination and partnerships between government and the private sector. Similarly, many agencies and departments have not

funded CIP efforts consistently across government. DoD began recognizing its need to consider critical infrastructure issues and proceeded somewhat independently and separately from other government agencies to focus on vital aspects central to DoD.

In 1997, DoD accelerated its exploration of dependencies on non-DoD infrastructures, standing up individual infrastructure sector teams and coordinating them through organizational processes such as the Critical Infrastructure Protection Integration Staff (CIPIS). Administrative and organizational efforts within OSD and the services were supplemented by operational initiatives, such as Joint Service Integrated Vulnerability Assessment (JSIVA) efforts, accelerated Red Teaming, DoD readiness exercises such as Eligible Receiver, and expanded infrastructure initiatives at the Joint Program Office for Special Technology Countermeasures (JPO-STC) and the Defense Threat Reduction Agency (DTRA). Most infrastructure vulnerability assessments focused on our key defense sites and facilities.

The risk environment, especially as it pertains to the critical infrastructures on which DoD relies, has changed. Threats to our homeland are becoming far more real, leading to important explorations of new risks: information warfare, biological and chemical warfare, and unconventional nuclear risks. While the risk environment has evolved, the infrastructures on which we rely, both domestically and in forward-deployed areas, have become more technologically advanced, concentrated in increasingly critical nodes, with complex distribution that DoD may not fully understand. Further, these infrastructures are less within the government's and DoD's control. Market pressures drive technological advancement within these networks, with fiscal realities no longer shaped by government needs.

The potential for a smart adversary to undermine the reliability or availability of our critical infrastructures is increasingly real. In the context of DoD's evolving Global Information Grid backbone, protecting information architectures and their content does not necessarily protect the underlying cyber and physical infrastructures. Similarly, protecting DoD's GIG within the gateways that connect it to private-sector-owned and -operated information infrastructures does not guarantee GIG availability should the leased connectivity outside those gateways be denied.

DoD should accelerate its efforts to identify its private sector dependencies and vulnerabilities, for DoD's information backbone as well as for other infrastructure dependencies that support energy requirements, logistics and transportation, water, and other critical infrastructure reliances. Without broad-based consideration of the full scope of critical infrastructure dependencies, mission constraints are unknown but potentially significant.

Relationship building and the resultant trust takes time. It is likely that both the government and private sector leaders at a localized level have multiple overlapping requirements and interests that contribute to both national security and the corporate prosperity of the infrastructure provider. For the purposes of critical infrastructure protection, it is important that these relationships advance toward the mutual benefits of government interests, including those of national security, and those of the critical infrastructure providers. Accordingly, it is important that efforts taking place at the local DoD installation level to define local dependencies on private infrastructures be explored and assessed in depth. More work needs to be done to identify vulnerabilities outside the lifelines of DoD, yet within the infrastructures on which DoD is very reliant.

Partnership between government and the private sector remains a vitally important yet elusive goal. Efforts to expand partnership with the private sector are hampered in many ways.

The private sector sees a lot of the government wrangling and interagency squabbles (some of these indicate the shortfalls in PDD-63 implementation), confusing the infrastructure owners and operators and making it easier to question the government's seriousness in partnering. Further, especially in the context of information sharing among government and the private sector, the owners and operators need relief from Freedom of Information Act (FOIA) to protect their proprietary data and interests and their competitive position.

Industry has indicated a willingness to help, but will not necessarily be motivated by the same things that motivate government. Industry fears regulation and unfunded mandates and will not go beyond what makes financial sense in the market economy. The private sector level of trust in government is low. In particular, the public is least trusting of three specific government sectors. They are law enforcement in particular, and to a lesser degree, the intelligence community and DoD. Government must be willing to openly respond to industry concerns if it hopes to overcome the hurdles in achieving partnership. While the government and the public perceive that industry has the answers, true partnering with industry remains the prime challenge. Best practices within the private sector and within government should be shared, not only as an element of trust and partnering, but to enhance the security and economic implications of infrastructure operability and assurance issues. Partnership challenges will become even more difficult in the future, as companies grow even more global.

FINDINGS

- There is a lack of understanding that it is not enough to simply protect one's own information systems. The DoD depends enormously on the commercially owned and operated telecommunications, transportation, electric power, and gas and oil industries, and on the financial sector.
- The level of trust in government is low. The outreach efforts by the government in the aftermath of PD-63 have not produced an outpouring of trust of government in the private sector.
- Industry has indicated a willingness to help, but will not be motivated by the same things that motivate the government. Industry fears regulation and unfunded mandates and will not go beyond what makes financial sense in the market economy.
- DoD is extremely reliant on private sector systems, networks, and infrastructures. Increased analysis is needed to pinpoint and assure vital reliances on the private sector.
- DoD must partner with the private sector to better protect networks and enhance national security.

RECOMMENDATIONS

- DoD should accelerate actions to identify critical infrastructure dependencies on the private sector – the DoD effort to produce sector CIP plans is a step in the right direction, but we would note that it is not moving along very quickly, primarily due to lack of funding.
- DoD must expand its interactions with the private sector and municipal providers of critical infrastructure services. This is best achieved on a localized level, between

base commanders (or other DoD leadership) and the infrastructure owners and operators. Direct DoD installation commanders (with support of JPO-STC) to identify critical infrastructure vulnerabilities, assess mission impact, and take corrective action with private sector service providers.

- DoD should work with Sector Lead Agencies to ensure that its requirements are incorporated into the information-sharing processes with the owners and operators of critical infrastructure.
- Advocate FOIA and other related legal relief to remove impediments to private sector information sharing.
- Fund and resource JPO-STC appropriately to support critical infrastructure assessments. As a minimum starting point, increase funding for such focused efforts to at least \$25M per year.
- DoD should modify or develop a process to assess the fiscal impact of infrastructure impact.

VI. SECURITY STANDARDS

During the course of this DSB Task Force, it became increasingly clear that, as with the definitional issues addressed earlier, understandings regarding use of information technology standards for desktop, system, and network security mean different things to different people--so much so that in the same organization responsible for promulgating the JTA, a new document, the Information Assurance Technical Architecture Framework (IATF), was developed for the purpose of setting forth guidance with respect to IA standards for the Global Information Grid (GIG).

The IATF document is a tutorial and collection of useful generic information on Information Assurance (IA). It should be noted, however, that the section of the IATF associated with standards and protocols for providing security to system applications is incorrect and inconsistent with the JTA.

The IATF, unlike the JTA, is not a standards setting or selection activity. Rather, the IATF Forum has been organized to encourage participation by vendors of largely commercial off-the-shelf (COTS) IA products and services. The major focus of the IATF is the development of protection profiles (under the Common Criteria [CC]) that will be used to evaluate products, e.g., under the National Information Assurance Partnership (NIAP) program operated by the National Intelligence Support Team (NIST) and the National Security Administration (NSA). There is no unified architectural underpinning for the IATF. This is to be expected, i.e., security evaluation criteria such as the CC (and product profiles based on the CC) tend to be architecture independent. As a result, the collection of standards cited by the IATF in their briefing to our panel lacks architectural continuity and it is not an appropriate alternative to the work of the JTA.

Many of the standards that are lumped together are experimental or dead. For example, S-HTTP is not implemented in any commercial browsers or servers; it lost the protocol battle to SSL/TLS. SPKI is not a standard, but rather is the experimental output of a failed Internet Engineering Task Force (IETF) working group, not supported in commercial products. The PKIX WG of the IETF produces standards based on X.509, which are implemented in a wide variety of products. Moreover, the other IETF security protocol working groups make use of the PKIX standards, not SPKI.

The IATF referenced a wide range of security labeling standards that are a mix of redundant and/or superseded documents. The IATF thus suffers from the same problems associated with the TAFIM; it is a collection of history and general information--not a document that can be used to implement interoperable, secured information systems for DoD. Figure 1 shows the numerous protocols issued as guidance in the IATF, most of which are inconsistent with the JTA.

Global Information Grid Standards & Protocols for Providing Security = Inconsistent with JTA

- | | |
|--|---|
| <ul style="list-style-type: none"> • Application Layer <ul style="list-style-type: none"> - Secure Hypertext Transfer Protocol (S-HTTP) * - Object Management Group's Common Object Request Broker Architecture (CORBA) - W3C XML Transfer Protocol - Secure FTP (S-FTP) - Secure Electronic Transactions (SET) - Message Security Protocol (MSP) - Secure/Multipurpose Internet Mail Extensions (S/MIME) • Transport & Network Layer <ul style="list-style-type: none"> - Transport Layer Security (TLS) - Secure Socket Layer (SSL ver 3.0) - Secure Shell (SSH) - Internet Protocol Layer Security (IPSec) • Data Link Layer <ul style="list-style-type: none"> - Point-to-Point Protocol (PPP) - Serial Line Internet Protocol (SLIP) | <ul style="list-style-type: none"> • Security Management Infrastructure <ul style="list-style-type: none"> - Internet Engineering Task Force (IETF) Public Key Infrastructure - IETF Simple Public Key Infrastructure (SPKI) * - IETF Domain Name System Security (DNSSEC) • Data Labeling <ul style="list-style-type: none"> - National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 188 Standard Security Label - Institute of Electrical and Electronics Engineers (IEEE) 802.10 g Secure Data Exchange (SDE) Security Label - IETF Internet Security Label - International Organization of Standardization (ISO) SC-32 Security Label - Military Standard (MIL STD) 2045-48501 (Common Security Label) - SDN.801 Reference Security Label - ISO MHS.411 Security Label |
|--|---|

Figure 1.

DoD policy requires that the Joint Technical Architecture (JTA) be used as the “building code” for the DoD information infrastructure. On the other hand, the recent document from the Deputy Secretary of Defense, “Department of Defense Chief Information Officer Guidance and Policy Memorandum no. 68510,” Department of Defense Global Information Grid Information Assurance (ASD/C3I), suggests that the IATF and published Common Criteria Protection Profiles be consulted “for guidance, and IA solutions to be considered to counter attacks.” A major concern is the apparent confusion these two policy statements could cause within the IA community.

There is an urgent need to provide JTA education to all personnel working with the GIG architecture. Though the IATF effort may be viewed as being helpful in several ways, such as documenting what is available in the commercial sector and what has not survived the “test of time,” the JTA should be positioned as the compelling document for guiding the use of standards within the GIG. Commercial standards should be used for security in the GIG wherever practical; however, there will be DoD-unique requirements for certain security implementations not available from the commercial sector. For this reason, we support the R&D/technology

initiatives documented in the Technology chapter of the DIO Task Force report as well as the recommendations put forth by the Architecture Panel of the DIO Task Force.

FINDINGS

- The IATF suffers from the same problems associated with the TAFIM; it is a collection of history and general information—the IATF is not a document that can be used to implement interoperable, secured information systems for DoD.
- The IATF standards are incorrect and inconsistent with the JTA and private sector practice.

RECOMMENDATIONS

- A clarification memorandum should be issued making it clear that the JTA will be adhered to for all GIG implementations, especially in the IA domain.
- The JTA is the better reference on IA standards and protocols, and it should be referenced as such in all GIG IA policy documents.

APPENDIX A. ACRONYMS

BIOSG	Bilateral IO Steering Group
CC	Common Criteria
CERTs	Computer Emergency Response Teams
CIAO	Critical Infrastructure Assurance Office
CIP	Critical Infrastructure Protection
CIPIS	Critical Infrastructure Protection Integration Staff
COTS	Commercial off-the-shelf software
DIO	Defensive Information Operations
DTRA	Defense Threat Reduction Agency
EO	Executive Order
EOP	Executive Office of the President
FOIA	Freedom of Information Act
GAO	Government Accounting Office
GC	General Counsel
GIG	Global Information Grid
I&W	Indications and Warning
IA	Information Assurance
IATF	Information Assurance Technical Architecture Framework
IETF	Internet Engineering Task Force
IC	Intelligence Community
IO	Information Operations
ISACs	Infrastructure Sector Analysis Centers
IWG	Interagency Working Group
JPO-STC	Joint Program Office for Special Technology Countermeasures
JTA	Joint Technical Architecture
JSIVA	Joint Service Integrated Vulnerability Assessment
NEC	National Economic Council
NIAP	National Information Assurance Partnership
NIPC	National Information Protection Center
NIST	National Intelligence Support Team
NSA	National Security Agency
NSC	National Security Council
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PDD63	Presidential Decision Directive
PRD	Presidential Review Directive

ANNEX B. PANEL MEMBERSHIP

Chairman:

Mr. Richard Wilhelm

Booz-Allen & Hamilton

Members:

Mr. Brenton Greene

Sandia National Laboratories

Mr. David Henry

Scitor

Mr. Owen Wormser

C3I

ANNEX E

**Defense Science Board Task Force
on
Defensive Information Operations**

Panel Report on Legal Implications

**REPORT OF FINDINGS,
DISCUSSION/OBSERVATIONS
AND RECOMMENDATIONS**

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
The Overlapping of National Security and Law Enforcement Missions	1
Why Information Sharing Is So Important	2
Why Information-Sharing Is So Hard	2
Recommendations for the Defense Department and the Justice Department	3
Recommendations for Congress	4
I. Introduction: Why Sharing Information About Network Attacks Is Important – and Hard to Achieve.....	7
II. Recommendations	11
APPENDIX A. Acronyms	A-1
APPENDIX B. Task Force Members	B-1

EXECUTIVE SUMMARY

"Yesterday, December 7, 1941 – a date which will live in infamy – U.S. forces in Pearl Harbor suffered numerous criminal trespasses. I have mobilized a team of prosecutors and FBI agents to investigate and take action."

In 1941, FDR never even considered giving that speech. Today, he might have to.

If critical U.S. information networks were attacked tomorrow in an "electronic Pearl Harbor," FBI agents and Justice Department prosecutors would in fact be on the front lines. Unfortunately, this report concludes, law enforcement and national security agencies have not learned to work together well to defend against attacks on U.S. information networks. Legal and cultural roadblocks have made it difficult for the Defense Department to rely on the FBI and Justice for full information about potentially dangerous attacks. This report proposes an agenda for new leadership and new compromises to break through these roadblocks.

THE OVERLAPPING OF NATIONAL SECURITY AND LAW ENFORCEMENT MISSIONS

Why have Justice Department entities like the FBI assumed such a large role in defending against network attacks? In a word, because attacks on American networks are typically the work of hackers, not foreign states. They are crimes, nothing more.

But that will change, and soon. Hackers' tools will become weapons in the hands of hostile nations, because U.S. information systems are a tempting target, especially for countries that cannot confront our armed forces directly. Network attacks are anonymous – or at least deniable. They are asymmetric. They allow hostile nations to pick a battlefield that minimizes American strengths in conventional and nuclear forces – indeed, one that turns strength into weakness by exploiting the United States' unique dependence on computer networks. The next Saddam Hussein – or the current one, for that matter – could win a symbolic victory just by tying up Manhattan traffic for a day. But some believe network attacks will soon be able to cause deaths and chaos across the country – especially if offensive capabilities continue to outpace our defenses.

In short, network attacks have a national security as well as a law enforcement dimension. DoD must be involved, both because it has a responsibility to defend the country and because it depends so heavily on a civilian infrastructure that is particularly vulnerable to network attacks. But DoD cannot act alone; it may not be possible to tell at the start of an attack whether the matter can be treated as a crime or an act of war or something in between. This means that the defense, intelligence, and law enforcement communities must be prepared to work together in a smooth and coordinated way.

Based on what the task force has seen, that day is a long way off. While they have been quick to take the lead in protecting information networks, the Justice Department and the FBI

have been slower to recognize the need for cooperation with the Defense Department and other national security agencies.

WHY INFORMATION SHARING IS SO IMPORTANT

This tendency toward limited information sharing has harmed the country's preparations for attacks on U.S. critical information infrastructure. The first order of business in preparing to defend against network attacks is to gather information about the attacks now being mounted against U.S. information systems. The more we know about today's attacks, the better prepared we will be to deal with tomorrow's. Information warfare cannot be launched blindly. Like any weapon, it must be tested. Indeed, to be most effective, information warfare should be planned and preliminary intrusions should be launched years before an overt attack – defenses must be probed, vulnerable systems reconnoitered, logic bombs planted. To judge the extent of the danger, we should be watching intently for just such activities – sifting those patterns from the noise of “script kiddy” hackers. We should be alert for the subtle signals that governments and terrorists are in fact beginning to turn the theory of information warfare into practice.

Thus, gathering information about the kinds of attacks now being launched is the crucial first step of any defensive effort. Unfortunately, this task has become the subject not of effective initiative but of continuing political and bureaucratic conflict. Although it has responsibility for national defense, the Defense Department must rely on law enforcement agencies such as the FBI and the Justice Department to gather information about network attacks and then decide what DoD needs to know. Thus far, however, the FBI and the Justice Department have been far too focused on their own missions to provide the kind of information sharing that DoD needs.

WHY INFORMATION-SHARING IS SO HARD

The FBI is the principal “intake point” for information about network attacks, in large part because it is easy to use the tools of criminal investigation to gather information about an attack, especially in its early stages. That is why the National Infrastructure Protection Center (NIPC) was housed within the FBI. Although staffed by defense and intelligence personnel as well as FBI agents, it relies heavily on criminal investigative tools that could not easily be deployed by other agencies.

But the effectiveness of NIPC in protecting national security depends on sharing information about attacks, and the FBI has a remarkably bad reputation on that score. A wide range of different communities – local police, intelligence analysts, civilian agencies, and business executives – all complain with regularity that however much information they share with the Bureau, the Bureau never reciprocates.

The NIPC has struggled to avoid the same reputation, but the culture of reticence cannot be turned on and off, particularly when the Justice Department, for its own reasons, has raised additional barriers to information sharing with defense and intelligence agencies. To some extent, the atmospherics surrounding the dialogue between the NIPC and the agencies it supports has made it difficult to arrive at ground truth, but the task force believes that what it has found warrants action. Without substantial improvement, the NIPC cannot live up to its initial promise.

As things now stand, DoD cannot count on NIPC, Justice, or the FBI for a free flow of information about network attacks. On the contrary, the task force identified numerous policies and legal interpretations at NIPC, the FBI, and the Justice Department that have prevented

effective information sharing about potential national security risks. The task force concludes that these barriers must be swept away, and soon, if DoD is to continue to support and rely upon NIPC. Unless NIPC, FBI, and Justice overcome their narrow crime-fighting perspectives – in a formal high-level agreement with the Defense Department – then DoD and the intelligence community should pull out of NIPC and create an independent center for gathering and sharing information about the most serious network attacks. This should, however, in the view of the task force, clearly be a measure of last resort.

RECOMMENDATIONS FOR THE DEFENSE DEPARTMENT AND THE JUSTICE DEPARTMENT

Rather than splinter the government's limited resources further, the task force recommends several specific changes in the policies and legal interpretations that have prevented NIPC from achieving its full potential as an information-sharing center. It is the view of the task force that the necessary changes cannot be achieved without leadership from the very top of both departments, and that the issues raised below should form the agenda for a series of talks that will, we hope, culminate in a new agreement over information sharing between the law enforcement and national security communities.

- First, all information available to NIPC should also be available to defense and intelligence analysts (who are already trusted with rather more sensitive information) unless there is an express legal bar on sharing or an *interagency* consensus that sharing the information is imprudent. The task force found that there may be misperceptions about the "law enforcement sensitive" label that is placed on information flowing from the NIPC to the Department. The Justice Department should clarify for the department that the label is attached to sensitize its readers rather than to prevent its flow to those requiring the information within the department. Likewise, the task force also believes that DoD agencies (including NSA) should share all available information on events with the NIPC.
- Second, the Justice Department has blocked NIPC from easy and natural communication with the National Security Council (NSC) about infrastructure attacks, despite the NSC's central role in national security decision making generally and infrastructure protection in particular. The DoJ is plainly reluctant to share information about criminal investigations with White House personnel, but DoJ's general policy, should not be applied to information about network attacks.
- Third, DoD should have access to information about network attacks gathered under Title III (the wiretap statute). The Justice Department opinion refusing to provide this access shows little appreciation of the need for interagency cooperation on national security matters and should be reconsidered.
- Fourth, concerns about grand jury secrecy have made it difficult to know what material in a criminal investigative file may be shared with DoD and what may not. These concerns are mostly derived from very conservative readings of the rules on grand jury secrecy (readings adopted in part to serve the prosecutors' interest in avoiding public disclosures of their investigative priorities). They are also derived in part from the Justice Department's failure to discipline investigators of infrastructure attacks. These investigators could gather information without using grand jury

subpoenas and thereby avoid later information sharing difficulties, but the FBI and Justice Department do not require their investigators to use these less problematic tools in the first instance. The rules on sharing grand jury information should be clarified to permit sharing for national security purposes; until this is accomplished, computer crime investigators should be prohibited from using grand jury subpoenas without interagency approval. While the amount of grand jury material that has been withheld is disputed, and may be relatively small, the failure to address this issue continues to create tension.

- Fifth, NIPC is buried so deep in the Justice and FBI bureaucracy that it cannot perform its interagency role effectively because it cannot assure its counterparts in other agencies that decisions can be rapidly referred to high levels in the bureau and the Justice Department. NIPC should report directly to the Office of the Director FBI as well as the Office of the Deputy Attorney General.
- Sixth, DoD has not taken all the steps necessary to ensure a large and strong contingent of DoD detailees at NIPC. Assuming a successful resolution of the issues raised in this report, DoD should upgrade its contribution to NIPC, both in numbers and in quality, and it should treat NIPC service as a "joint" appointment for purposes of military promotion.
- Seventh, NIPC has much to offer DoD on questions such as when to block a particular hacker from further access and when to let the hacker continue in an effort to learn more about his techniques and purposes. DoD should agree on a role that clarifies NIPC's purely advisory position while guaranteeing that NIPC has a voice in such decisions. DoD should further clarify the commander's decision-making authority in this area so that responsibility is unambiguous.
- Eighth, NIPC and the Justice Department's computer crime experts have exceeded their jurisdiction in trying to limit what information intelligence agencies may receive; neither NIPC nor the Justice Department's Criminal Division should have a role in deciding whether and how DoD entities share information with NSA or other intelligence agencies.
- Finally, the task force notes that "red team" exercises, though vital, have been slowed in the past by multiple legal signoffs and supervision at DoD. This concern is diminishing as red teaming becomes more common, but it remains true that a standardized and simple set of procedures should be adopted to allow unannounced "red team" attacks on all DoD networks without excessive high-level intervention by DoD officials.

RECOMMENDATIONS FOR CONGRESS

All of the recommendations above could be implemented without changing any statute. That is the preferred solution. Nonetheless, there are areas in which U.S. laws have failed to anticipate the need for effective critical infrastructure protection. For that reason, the task force

recommends that the Defense Department support a variety of relatively limited changes in existing law.

- Most important, DoD should have its own civil authority to seek information about network attacks with national security implications. Under existing law, network service providers may give away information about hacking attacks on street corners, but they are legally prohibited from giving the information to a government agency unless the agency begins a criminal investigation. This is unfortunate for all. It forces hacker investigations into a criminal posture, which is likely to be bad for the hacker as well as for the opportunity to share information among agencies. The government should justify any request for information about its citizens, but it should not have to launch a criminal investigation before it can gather information needed to protect national security.
- Second, the task force encountered a disturbing limitation in the ability of the government to maintain wiretap coverage of persons engaged in long-term hacking campaigns against government networks. Ironically, the more likely it is that the attackers are sponsored by foreign governments, the less likely it is that wiretap coverage will be maintained, because the likelihood of successful prosecution will decline over time. In the end, criminal wiretap authorities are inadequate for this problem, and a statutory solution should be sought that protects both national security and the civil liberties of Americans. One possibility is a provision denying network trespassers an expectation of privacy for their actions in attacking a victim's information system.
- Third, current law concerning "trap-and-trace" orders often requires that law enforcement agencies seek multiple, sequential orders as they trace a single hacker from system to system. This provision should be modified to allow a single, nationwide order aimed at a single attacker who uses multiple computer systems. In addition, there is currently no statutory provision allowing the government to obtain certain types of information without the requisite order in situations of extreme urgency. This is an oddity, since under the Electronic Communications Privacy Act, wiretaps may be initiated without a judicial order in an "emergency situation." In the interest of enabling law enforcement officials to obtain the crucial information they need for the prompt investigation of critical infrastructure attacks, the provision allowing emergency wiretaps should be extended to court orders and subpoenas as well.
- Fourth, if agreement cannot be reached with the Justice Department concerning the Title III and grand jury rules that currently restrict information sharing with DoD, Congress should clarify its intent that the confidentiality of criminal investigations not trump the national security interests of the United States.
- Finally, though the majority of the problems outlined here focus on information-sharing deficiencies between and among government agencies, greater efforts could be made to encourage voluntary private-sector cooperation in hacking investigations.

To this end, the use of nondisclosure agreements in gathering information on network attacks should be expanded, and narrowly tailored legislation that would restrict the Freedom of Information Act disclosure of information shared pursuant to a hacking investigation should be considered.

I. INTRODUCTION: WHY SHARING INFORMATION ABOUT NETWORK ATTACKS IS IMPORTANT – AND HARD TO ACHIEVE

Like everyone else in America, the armed forces depend heavily on sophisticated communications networks – not just their own, but those of the civilian industries that support them. U.S. adversaries know this. That is why information warfare attacks on our networks are a near certainty – because they are likely to work. How great is this risk? We do not know, and this panel report focuses on what we don't know, and why.

We do know that attackers have had disturbing success in penetrating sensitive systems essential to carrying out the Defense Department's mission. Worse, the attackers who have succeeded are mostly vandals and petty criminals, and the tools they have used are offshoots of existing technology. But no one estimates the military might of the United States by studying the weaponry of American street criminals, and by the same token, the technology of information warfare will soon bear little resemblance to the viruses and denials of service that currently annoy Internet users. The problem is likely to get worse before it gets better.

Better information about network attacks is the first line of defense. To launch a serious information warfare attack on the United States would likely require considerable preparation – probing defenses, testing tactics, leaving behind logic bombs or back doors. If the government is to have warning of future attacks, it needs to gather information about current attacks in a systematic way and to analyze the information for patterns.

While gathering and sharing information on attacks is the foundation of a defense against information warfare, so far we do it badly. The private sector is reluctant to share information for both competitive and legal reasons. Information sharing comes no more easily to government. Intelligence agencies classify information in order to limit sharing to those with a "need to know." Law enforcement agencies restrict sharing to protect witnesses and keep their targets in the dark. And almost everyone in government treats information as currency, to be offered only sparingly and in return for value.

In short, sharing information does not come naturally. Despite this reluctance, the need to centralize and share information about network attacks is so obvious that an interagency entity, the National Infrastructure Protection Center (NIPC), was created to do just that.

Specifically, NIPC has two primary practical goals. One is to investigate (and, wherever possible, prevent) attacks on critical infrastructure systems. Critical infrastructure systems are the backbones that allow U.S. cities and towns to function; they include the electrical power grid, the water works, and the telecommunications pipelines. Half of NIPC's mission is to coordinate the collection and dissemination of information about the security and defense of these systems. The other part of NIPC's mission is to coordinate the sharing of information on network attacks within the law enforcement and intelligence communities, which includes, of course, DoD.

When NIPC was established, there was some debate about where it should be housed. Agencies like the Commerce Department were rejected because they lacked independent

investigative and intelligence capabilities. Intelligence agencies were rejected because their mission is focused on foreign countries, and their capacity to gather intelligence on Americans is rigorously limited. While information warfare itself is an entirely appropriate concern of the intelligence community, most network attacks are not state-sponsored. Indeed, the thousands of hackers whose activities obscure the acts of foreign governments are as likely as not to be Americans. By the same token, while DoD is the proper agency to respond to information warfare, it has little or no authority to deal with simple vandals.

Given those constraints, it seemed that the logical "intake point" for information about infrastructure attacks was the FBI, which has authority to investigate both common criminals and foreign agents. Despite this logic, the FBI was a controversial choice. It was handicapped by a remarkably deep and pervasive reputation – among other law enforcement agencies, in the intelligence community, and in the private sector – as a black hole for information. Everything goes into the Hoover building, according to this view, and nothing comes out.

For that reason, many steps were taken to keep NIPC from falling heir to the FBI's reputation for restricting information. A well-regarded Justice official was transferred to head the office, and detailees from the Defense Department and intelligence agencies were put in charge of information-sharing offices within NIPC. Based on what the task force learned in the course of interviewing numerous DoD, Justice, NIPC, and intelligence sources, however, this was not enough. Putting information-sharing responsibilities in the hands of law enforcement agencies has produced serious problems that were not adequately foreseen when NIPC was established.

Because of legal and cultural restrictions, NIPC staff, even personnel detailed from DoD itself, have found it difficult to share information about network attacks in an easy, cooperative fashion with agencies outside law enforcement. The problems have been many. The National Security Council, for example, has been denied timely information on the status of network attacks under investigation; whole categories of information (Title III intercepts, for example, and materials obtained via grand jury subpoena) have been set aside by the Justice Department as the domain only of law enforcement agencies. Other information has been designated as "law enforcement sensitive" and subjected to dissemination restrictions in a fashion that lacks the safeguards usually relied upon to prevent overclassification.

Of course there are explanations for all of these roadblocks, and in many cases NIPC has worked to overcome them and to establish at least the beginnings of an effective information-sharing facility. The task force does not underestimate that achievement. NIPC has faced pressures from many directions other than defense and the intelligence communities. Businesses, civil liberties advocates, competing law enforcement agencies, and even foreign governments have all claimed the right to help set one or another aspect of NIPC policy, though they have been notably more reticent when resources have to be put into the effort. In these circumstances, to create a functioning entity with its own esprit has proved to be no easy task.

That said, the task force finds it unlikely that NIPC, operating under current constraints, can consistently provide the kinds of information needed by DoD to protect against attacks with a national security dimension. NIPC is still far too dominated by the law-enforcement culture and by legal interpretations by the FBI and Justice Department that tend to reinforce the NIPC's reputation for not sharing information. While NIPC has managed to work around some of these obstacles, the current structure for sharing network attack information still is not responsive enough to the interests of national security and intelligence agencies.

This situation is not tolerable, particularly for the Department of Defense. To a very great extent, DoD depends on NIPC for the information it needs to defend itself and the nation. Reliance on law enforcement agencies for such a crucial element of support will only work if those agencies seamlessly share with DoD any and all information likely to have a bearing on DoD's defense mission. Current policies suggest that the FBI and Justice Department are not willing (or perhaps think themselves unable) to share information in this seamless way. The restraints on NIPC have significantly restricted its ability to play an adequate interagency information-sharing role.

The task force provided early drafts of conclusions to NIPC, and NIPC strongly, sometimes stridently, disagreed with task force conclusions on this point. NIPC says that it has managed to find ways to share virtually every useful piece of information about network attacks that has come into its hands. While the doctrines and difficulties laid out in this report are acknowledged as obstacles, NIPC believes that in the end they can all be overcome – indeed that almost all have been overcome – with creativity and care. NIPC urges us to focus on its successes and its need for substantial additional resources from DoD to conduct the necessary analyses of data already being shared.

The task force agrees that there have been successes, and that more analytic resources are needed – at NIPC or elsewhere. But that does not alter the fact that substantial legal and policy roadblocks exist, and that those roadblocks have prevented sharing already. Change will not come quickly. While in some cases NIPC has worked around the problem successfully, we must not wait until there is a catastrophic failure to address these concerns. The legal and policy issues identified here are continuing threats to the effort to build a seamless and effective information-sharing system for network attacks.

The task force recommendations go to the heart of this concern.

II. RECOMMENDATIONS

RECOMMENDATION I:

DoD Should Insist on a High-Level Agreement with Justice and the FBI that Reforms NIPC's Role and Structure.

Part of the information sharing problem has been a lack of clear leadership. After the initial cabinet-level activity to establish NIPC, little high-level attention was paid to how preparations for information assurance were actually functioning. In that atmosphere, each agency asserted its prerogatives without much fear of oversight. Issues related to information sharing practices were not readily resolved because political decision makers did not intervene to force reasonable compromises in the interest of NIPC's overall mission.

The task force's central recommendation, therefore, is that this problem be addressed at the highest levels of the Justice and Defense Departments, and that DoD insist on major changes in exchange for augmenting its support for NIPC.

Currently, DoD is the largest contributor to the staffing of NIPC, other than the FBI itself. Present staffing levels at NIPC are roughly as follows:

FBI:	82
DoD ¹ :	14
United States Postal Service:	1
CIA:	2
Energy Department Labs:	1
Local Law Enforcement:	1
Foreign Liaisons:	2

There is no high-level agreement between DoD and Justice/FBI about the terms of details to or the information-sharing practices of NIPC. Instead, information-sharing policy is set by a two-page memorandum of understanding (MOU) that is to be signed by DoD, FBI, and each detailed employee. The MOU is an inadequate and entirely one-sided document, essentially imposed on the detailees and their agencies. Some provisions are unexceptionable – such as those making clear that each employee sent from DoD will be tasked exclusively by his or her superiors at NIPC, will be removed from the chain of command in DoD, and will have access to information in FBI files and to other sensitive information.

Unfortunately, the MOU goes further. It requires that dissemination of information from NIPC, including dissemination back to the detailee's home agency, be governed by FBI policy as well as applicable statutes and other guidelines or procedures.²

¹ The DoD elements represented include NSA, NCIS, Air Force OSI, DCIS, air force, army, navy, and OSD.

² NIPC argues that the MOU is necessary to protect against claims that DoD personnel are acting in violation of *posse comitatus* rules and that NSA and CIA personnel are violating rules governing intelligence agency handling of U.S. person information. This is open to question, and should be more carefully reviewed. In practice, *posse comitatus* is rarely a bar to assistance to law enforcement, and while intelligence agency restrictions may require intelligence personnel on detail to obey the laws governing law enforcement, it is not clear that these personnel must submit to additional and unspecified

Those policies are by no means limited to information-sharing restrictions imposed by law. It is of course understandable that anyone handling law enforcement information would be subject to any restrictions imposed by law on the use of such information. But the MOU goes beyond that to impose sweeping restrictions that are not required by law. Such a sweeping approach is inconsistent with NIPC's mission and with the participation of other agencies in that mission. Some restrictions based on law enforcement policy rather than law may well be appropriate, but the burden of identifying and justifying each separate restriction should be on the FBI and Justice. (It is not enough in an interagency context, to say, as NIPC has, that equivalent restrictions are imposed on FBI personnel. The point of an interagency task force is that the personnel bring different skills and traditions to the task.)

Agencies that detail staff to NIPC still pay the salaries of their detailees. It makes no sense to pay those salaries unless the employees' participation in NIPC provides ongoing value to the agency that details them. Potential restrictions on detailees' communications limit their value to the sending agency. Some agencies are already cutting back their participation. The Secret Service, for example, has ended its participation. After initially insisting on sending seven people, it has pulled all of its representatives back, in part because of reluctance to accept FBI information-restriction policies. The Department of Energy has also failed so far to replace one of its detailees; it too has had conflicts with the FBI and NIPC over information sharing.

Although DoD originally planned to send eighteen detailees, only fifteen have ever been assigned to NIPC, and the likelihood of replacement once they rotate to a new assignment is uncertain. Some DoD elements, notably the National Security Agency, have also had conflicts with NIPC over information-sharing policy; NSA's participation in the NIPC, as well as that of the CIA, has been sporadic. With this track record as a backdrop, it is at least fair for the NIPC to make the claim that pulling back detailees by agencies, as well as sporadic participation, will indeed hamper the NIPC's efforts at information sharing.

Currently, the participation of other agencies, including DoD, is dwarfed by the contribution of the FBI itself to the office's staffing and funding. This will soon turn NIPC into an FBI office rather than an interagency office, and that will have a serious impact on all aspects of the operation. (NIPC's preferred solution would be to increase staffing from other agencies. The task force agrees, but this will happen only if information-sharing problems can be solved.)

DoD should not follow the example of the Secret Service and simply decamp – at least not without attempting to negotiate a broader and more reasonable framework agreement with Justice and the FBI. The task force does not believe that NIPC's problems are necessarily fatal, or that a "go it alone" approach is a better solution for DoD. NIPC continues to be the best window into law enforcement information about network attacks. While its reputation in the private sector is decidedly mixed, it does obtain important information from cooperating companies as well. And so many network attacks are ultimately of little practical interest to DoD that it should allow other agencies to take the lead in addressing them. Withdrawing from NIPC would run a risk of weakening both NIPC and DoD. If possible, it would be far better to

NIPC and FBI policies on handling law enforcement information. Moreover, the FBI required other law enforcement agencies – such as the United States Secret Service – to abide by the same agreement, even though *posse comitatus* was not an issue. Indeed, the Secret Service balked at signing the MOU, because it was unduly restrictive, believing as we do that there was no sense in agencies detailing personnel if the detailed employee could not share information more freely with his or her agency of origin.

reform NIPC to make it truly interagency in spirit rather than a captive of law enforcement policies.

While information-restricting law enforcement doctrines need to be addressed in any framework agreement, they are not the only issues that should be covered in high-level talks between DoD and Justice. DoD's own practices in sharing information and choosing detailees are appropriate matters for concern on the part of NIPC. So too is the current placement of NIPC within the FBI hierarchy, which hinders the functioning of NIPC as a truly interagency body.³ Finally, there is no written agreement on NIPC's role in such obvious questions as whether it is better to lock a particularly dangerous intruder out of a system or to let him in and watch him in the hopes of learning what damage he is capable of causing.

Drafting an agreement that covers all of these aspects of NIPC's operations may be the only way to engage the attention of decision makers within DoD and Justice/FBI, and to ensure that NIPC's critical early-warning mission will be given higher priority than each agency's turf concerns.

The remainder of this section recommends specific reforms that the task force believes should be incorporated into a framework agreement between DoD and Justice/FBI.

RECOMMENDATION 1.1:

All information held by NIPC about infrastructure attacks should be available to DoD unless sharing the information would violate a legal prohibition. DoD should provide similar assurances for information in the hands of its agencies.

Neither NIPC nor DoD has been a model of information sharing. Complaints about unnecessary barriers to information sharing can be heard in both camps, and with good reason: in each agency, there are cultural limits to information sharing. Nonetheless, the task force judges the problem to require more attention on the NIPC side, primarily because that is where the information about network attacks is being centralized.

It is easy to understand the sensitivity of some law enforcement information. The name of a suspect, the identity of a source inside a criminal organization, the effectiveness of a particular investigative technique – this kind of information is jealously protected by law enforcement agencies. Indeed, NIPC fears that if FBI agents were told that NIPC intended to distribute such information throughout the government, they would stop talking freely to NIPC, leading to a new wall between the FBI and other agencies – but this time with NIPC on the other side of the wall.

NIPC has tried to satisfy law enforcement concerns while at the same time finding ways to share information with others. In general, it uses two methods. First, it sanitizes its reports to remove the most sensitive law enforcement sources and methods while still providing useful information. Second, it supplies information marked "law enforcement sensitive," a designation

³ Concern has been expressed at DoD that, in the latest reorganization, NIPC has found itself "buried" in the terrorism division of the FBI. Treating NIPC like any other FBI program heightens the impression that it is simply an FBI office that happens to benefit from free labor provided by other agencies. It is also difficult to run an interagency process that, when complete, must climb the FBI and Justice bureaucracies through several levels. This issue is not without its difficulties. Viewed as a "line" office, NIPC is not big enough to be an FBI division by itself, and so giving it a direct report to the Office of the Director would require treating it more like the FBI staff offices, such as Office of General Counsel.

that is similar to the designation "Originator Controlled (ORCON)" in the classified world, telling readers that the information may not be further circulated without the approval of the originating agency. According to NIPC, including the CIA detailee in charge of information sharing, these methods have allowed NIPC to share practically everything of value to other agencies.

NIPC sees the use of the "law enforcement sensitive" concept as a valuable tool that favors sharing. The task force is more troubled by it, particularly because the doctrine is both vague and broad. As set forth in a more detailed NIPC protocol on information sharing procedures, dissemination may be limited to shield "a protected source, sensitive method, [or] confidential witness," categories where restrictions might be justified if interpreted narrowly. But the protocol also protects even broader and more questionable categories of information, such as information identifying juvenile suspects, or information about cases that are awaiting trial. Even information in cases that have been closed can be restricted if the investigating agency thinks disclosure would compromise its sources and methods.

Understandable as the concerns of law enforcement may be, they do not justify such a broad set of restrictions – especially if the interpretation is left solely to law enforcement. Such a decision-making process lacks checks and balances. It does not utilize the more recognized (and in the view of the task force, more disciplined) classified information system familiar to national security agencies. And it makes law enforcement agencies the final authority in disputes about information sharing. The task force welcomes NIPC's assurance that the doctrine is rarely used to prevent sharing of relevant information. If so, it should be possible to adopt a default rule that calls for sharing in the absence of specific factors – and that allows DoD to participate in the decision about whether sharing is justified.⁴

In the task force's view, sharing of information about serious attacks should be automatic unless the sharing would violate a specific legal ban (such as Rule 6(e) of the Federal Rules of Criminal Procedure, which prohibits the sharing of grand jury information) or unless there is an interagency determination that the risk of compromising sources and methods requires the restriction. The task force discusses in later recommendations ways to minimize the adverse effects of legal restrictions on sharing. The recommendation that the risk of compromise be weighed against the value of the information bears further discussion here.

It is worth remembering that the principal justification for the "law enforcement sensitive" doctrine is preventing the compromise of a current or future criminal investigation. And it is obvious that this is a severe risk in some criminal contexts: investigations of organized crime, for example, are susceptible to compromise with consequences that can be fatal for the investigators. But the likelihood that sharing NIPC information with DoD will have such effects is vanishingly small, particularly because NIPC will have information mainly, if not exclusively, about criminal investigations of hackers, who are not known for bribing officials to gather intelligence or for adopting the other techniques of organized crime. More importantly, there is no reason to think that sharing NIPC information with DoD officials is more risky than sharing the information with criminal investigators or prosecutors. DoD is entrusted with far more serious secrets than a

⁴ NIPC has pointed out that DoD and other agencies do, in fact, have detailees at NIPC, and some of these detailees are already in a position to approve dissemination of information that is law enforcement sensitive. This is a good thing, but it is not the same as giving DoD an institutionalized voice in the decision.

handful of investigative details in a hacking case, and its record of protecting secrets is at least as good as the FBI's and the Justice Department's.⁵

In fact, NIPC does not defend its restrictions on strictly law-enforcement grounds. It argues that the risk of compromise extends not only to individual criminal investigations, but also to general investigatory techniques, many of which are likely to be important to DoD as well as law enforcement. In these circumstances, the issue more closely resembles a classic intelligence "sources and methods" problem, and the usual tactics employed by the intelligence community to solve such problems should work.

It is for this reason that the decision as to whether to share information about an investigation should not be made exclusively by prosecutors and investigators. DoD must be given a voice in that decision, perhaps by designating an official from the Office of General Counsel who would always be trusted with investigative information as part of the interagency sharing process. (The task force notes that twenty-five years ago, intelligence agencies objected to the involvement of the Justice Department in their activities because they feared that prosecutors would be unable to protect intelligence sources and methods; those concerns have now been resolved by long practice. That prosecutors and investigators fear for the security of their special secrets is equally understandable -- and equally wrong.) Involvement of decision makers with different perspectives is an important guarantee of objectivity, but in the end the important thing is not just the process itself, but the principle that those who want to restrict information sharing must justify that view to other parts of the government. The default should be that the information is available to DoD and its agencies.

A second reason often advanced for not sharing investigative information is privacy. This report will address statutory privacy protections separately, but even where statutory restrictions do not apply, the task force agrees that protecting privacy is an important value that NIPC and other agencies need to bear in mind at all times. At the same time, it is worth remembering that NIPC can only share information about private citizens that it already possesses -- in other words, information that is already in the hands of at least one and probably several government agencies. It is reasonable to question how well privacy is protected by keeping information that has already been widely shared within the law enforcement community out of the hands of Defense Department analysts. A more effective protection would focus on preventing misuse by all the parties that have access to the information.

As stated at the outset, in focusing on the barriers to information sharing that have been erected at NIPC, the task force does not mean to suggest that this practice runs only one way. NIPC has cited its own examples of information withheld arbitrarily by NSA and perhaps other DoD elements. NSA and NIPC are seen as competing for similar missions and resources, and as is typical in such cases, each side has a store of grievances against the other. The task force recommends that DoD and its elements also make binding assurances that information will be shared with NIPC unless it is subject to legal restrictions. Both parties should ensure that NIPC personnel have clearances that are adequate to facilitate this information sharing and that there is a process for resolving disputes about which classified information may be shared with NIPC.

⁵ In rebuttal, NIPC and Justice point to an occasion on which a high-ranking DoD official briefed an ongoing attack and investigation to Congress only to have details leak to the press. This of course is unfortunate, and it has happened too often to every agency that depends both on secrecy and on Congressional favor. But every agency tends to remember the times when other agencies have been the source of a leak and to forget those in which it was the source. Keeping information away from DoD is not an appropriate solution to the problem of "political" leaks.

RECOMMENDATION 1.2:

NIPC should share all information about network attacks with the National Security Council and its staff unless the information is likely to compromise an investigation of a White House official.

If NIPC is to participate in national security planning and decision making, it must obey the same rules as other participants in that process. This includes providing all necessary information to the interagency process administered by the National Security Council (NSC). Currently, NIPC is unable to do so – a serious handicap that should be cured either by agreement between DoD and the Department of Justice or by the President.

Restrictions on FBI communications with the White House were imposed in 1994 in an agreement between the White House Counsel's Office and the Office of the Attorney General. Under that agreement, the FBI may not provide any information to a member of the White House staff except with the approval of the Deputy Attorney General (DAG). The purpose of this restriction is to prevent actual or apparent White House interference with or influence over criminal investigations. The arrangement gives the Deputy Attorney General an assurance that he is fully aware of any communications between the FBI and the White House.

In the context of NIPC, this restriction on sharing information is dysfunctional. During the Clinton Administration, defense against foreign-based infrastructure attacks was coordinated by a senior NSC official. Delaying the delivery of information to the NSC is not good management, and NIPC itself has asked Justice to modify the rule in this context, so far without effect. The NSC is a well-established mechanism for coordination of national security issues with interagency dimensions. In their defense, the Justice Department and NIPC emphasize that in the end practically everything the NSC wanted to know was provided by NIPC. The task force found that, on some occasions, the transfer of information to NSC has gone smoothly – as one official told us, "DAG approval can take 20 minutes." But in other cases, there have been significant delays in delivering information to the National Security Council due to disagreements between Justice and NIPC over what information should be supplied to the national security staff. Justice officials said they sometimes felt forced to choose between having their best technicians respond to attacks and having the technicians respond to what they called "drive-by tasking" from the NSC.

The task force did not try to decide whether NSC had asked for unnecessary or burdensome briefings, although it was noted that this is a widely held view at NIPC and the Justice Department. But even if that view is correct, Justice should not have responded by claiming the legal right to withhold information from NSC. DoD depends on the NSC to address interagency issues that arise when national security is threatened. The NSC process is well-oiled and has functioned predictably in a host of conflicts, and NSC is the logical place to address network attacks with national security implications. If agencies can refuse to provide information to that interagency process, they will always be tempted to withhold information that makes them look bad. Again, the default should be in favor of sharing information. In the long run, busy NSC officials are unlikely to ask for information that is not relevant to their jobs.

What of the concern that led to the no-White-House-briefings rule in the first place? The task force does not denigrate the concern that White House communications can lead to charges

of interference in a criminal investigation. For that reason, the task force agrees that NIPC should be free to refuse to provide information that would compromise an investigation of White House staff. But there is little reason to use a broader rule in this context. Criminal investigations of hackers will often have national security dimensions. So far, however, no one has raised the slightest suggestion of political interference. Until the risk of politicization of network investigations is something other than theoretical, this restriction should be lifted.

This change could be accomplished by a blanket approval by the Attorney General for the sharing of information on attacks with national security significance. But such approval has not been forthcoming, and it therefore should become the subject of high-level agreement between DoD and Justice.

Once again, the task force notes that this restriction falls into a pattern, in which FBI and Justice entities that are tasked with interagency responsibilities attempt to justify restrictions by saying that they are simply applying the Justice/FBI rules that usually apply to "criminal investigations." That is precisely the problem: these investigations are not exclusively matters of concern to prosecutors and investigators, and they cannot be treated as though Justice Department policies are the beginning and end of analysis. Unless the "business as usual" mentality at Justice and the FBI can be shaken loose in some form of agreement, DoD will have to create its own, separate capabilities, free of parochial constraints imposed for law enforcement reasons.

RECOMMENDATION 1.3:

Title III intercept information should be shared with DoD for purposes of assisting DoD in preventing attacks on its computer networks.

Sooner or later, usually sooner, any serious investigation of a network attack requires a wiretap. This allows investigators to intercept the communications between an attacker and the sites the attacker uses to launch (or launder) his attacks. Electronic intercepts are a fundamental tool in combating network attacks. But as things now stand, they usually can only be performed as part of a criminal investigation using the authority conveyed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. (Foreign intelligence intercepts can also be used inside the United States, but only if the target is an agent of a foreign power – something that is difficult if not impossible to determine at the outset of a hacker investigation.)

Use of criminal wiretap authority is in some respects easy. Hacking into other people's computers is a crime, so that the prerequisites for a Title III intercept order for data may be quickly met. But there's a catch. Once the data has been gathered under a Title III order, it may not be shared with DoD or other national security bodies. At least that is the view of the Justice Department, which interprets Title III as prohibiting such sharing. In the task force's view, the Justice Department's reading of Title III is at best arguable, and shows far too little concern for national security.

The statutory language in dispute is not lengthy. Under Title III, information derived from an intercept may only be used "to the extent that such use is appropriate to the proper performance of [the] official duties" of the law enforcement officer who has obtained the information. (*See* 18 U.S.C. § 2517 (1) and (2)).) This language would not bar DoD from receiving Title III information if "the official duties" of law enforcement officers include

protecting national security and preventing additional crimes. At one time, the Justice Department's Office of Legal Counsel (OLC) took a similarly broad view of the "official duties" language, concluding for example that the Justice Department could provide Title III information to congressional committees on the theory that responding to congressional inquiries is part of a government employee's "official duties." No longer -- after considerable delays, the OLC has recently issued an opinion that overrules its earlier interpretation and concludes that Title III authorizes only sharing of intercept information for official *law enforcement* uses.

The OLC opinion further concludes that this ambiguous intent is not overcome even by the National Security Act, which expressly grants the Director of Central Intelligence "access to all intelligence related to the national security which is collected by any department, agency, or other entity of the United States." (See 50 U.S.C. 403-4(a)(1994)). Finally, it dismisses a Reagan-era executive order directing all agencies to give the director of Central Intelligence "access to all information relevant to the national intelligence needs of the United States." (See Executive Order 12333 (1981))⁶

In the view of the task force, the OLC opinion is questionable as a matter of statutory construction, and it almost willfully ignores the national security implications of its conclusions. A careful reading of the law, as well as strong public policy concerns, argue in favor of the disclosures at issue here. OLC's contrary decision casts real doubt on the willingness in the Justice Department to give due weight to Defense Department interests when carrying out missions that mix national security and law enforcement.⁷

The OLC opinion suggests that it is appropriate to lean against sharing of Title III data because of privacy concerns. Privacy is indeed important, but as noted earlier one may wonder: will the targets of Title III wiretaps really be comforted by the knowledge that the contents will be provided to prosecutors' secretaries, perhaps even to IRS auditors -- but not to defense and intelligence authorities? There is of course an extra bit of privacy in any restriction on distribution of private information, but it is difficult to agree with the Justice Department's decision to treat this relatively minor gain for privacy as more important than the significant loss in terms of national security. The additional privacy benefit is particularly attenuated in the context of hacker intercepts. What makes classic wiretaps so troublesome from a privacy perspective is that they capture often-intimate conversations between parties who trust each other and believe their conversations will remain private. But intercepts of hacker attacks are typically focused on signals sent by the hacker to a victim's computer. The tap simply provides a quick

⁶ We should note that this opinion was resisted by NIPC on grounds that it is unnecessarily restrictive, while at the same time one of the principal OLC contributors to the opinion is now part of the office of the DoD General Counsel.

⁷ Other aspects of the opinion do little to dispel this view. For example, OLC determines that intelligence agencies will be allowed access to intercepts in one circumstance -- when they have been firmly subordinated to law enforcement and are simply putting their resources at the disposal of prosecutors and criminal investigators. *Then*, the opinion declares, there is no problem with sharing intercept information. In short, if the Justice Department's interests are served by sharing, the sharing is legal; if not, not.

The opinion also contains a remarkable passage to the effect that if a law enforcement intercept produces urgent national security information, then the President can order that it be shared with intelligence agencies. Given the National Security Act and Executive Order 12333, one might think that Congress had already authorized such an order and that the President had already issued it, but having rejected that obvious conclusion, the opinion is forced to find that the President has retained some inherent authority to order such sharing anyway, but that the authority should only be exercised in desperate circumstances. The opinion takes a convoluted course to arrive at a position that could have been achieved by giving a straightforward reading of the National Security Act.

way to capture keystrokes that are themselves part of the crime and that would not qualify under most people's definition of a communication, let alone a communication entitled to the highest possible privacy protection. These keystrokes may well be protected by Title III, but it is difficult to justify expanding their protection in the face of a law and an executive order that clearly require the Justice Department to share any intelligence relating to national security.

An OLC opinion is binding on the executive branch, but interpretations can be overturned, as this one overturned an earlier decision. The task force urges that the opinion be reconsidered in the context of a broader agreement on NIPC's information-sharing policies.⁸

RECOMMENDATION 1.4:

Rule 6(e) on sharing grand jury information should be clarified to permit sharing for national security purposes; until this is accomplished, computer crime investigators should be prohibited from using grand jury subpoenas without the express approval of NIPC, acting with interagency agreement.

Unfortunately, Title III is not the only criminal provision that prevents defense and intelligence agencies from gaining the full benefit of information obtained by criminal investigators about network attacks. Another provision with an impact on information sharing is Rule 6(e) of the Federal Rules of Criminal Procedure, which provides that attorneys for the government "shall not disclose matters occurring before the grand jury, except as provided for in these rules." Specifically, information may only be disclosed when permitted by the court, or to an attorney for the government or to "such government personnel ... as are deemed necessary by an attorney for the government to assist an attorney for the government in the performance of such attorney's duty to enforce federal criminal law". (See Rule 6(e)(3) (A) and (C)).

Unfortunately, the Justice Department has taken a narrow view of its authority to share information under this rule. To make matters worse, NIPC has taken an expansive view of what materials are covered by the rule. And, finally, Justice Department prosecutors continue to use grand jury subpoenas where other processes could be equally effective, unnecessarily expanding even further the body of material to be withheld from DoD and other agencies.

This report examines each of these three concerns separately. But first, it may be worthwhile to note that grand jury secrecy, while often praised as a protection for criminal suspects' privacy, actually serves the prosecutors' interests at least as well as the defendants'. The privacy rationale is that grand jury secrecy protects those who are investigated and not indicted, or not

⁸ If this cannot be done, we suggest that NIPC and the Justice Department maximize "parallel sourcing" of information that might otherwise only be obtained through the use of Title III. For example, some information produced from a wiretap targeting a hacker would also most likely be available directly from the computer of the victim, particularly once monitoring software was installed. We recognize that this is not a complete solution; if all the information produced by a wiretap could be harvested in another fashion, the wiretap would not be approved, since by law an intercept can only be used with necessity. Nonetheless, procedures to automate and make routine such parallel sources are worth considering. (Even this limited solution creates new difficulties, however. While systems administrators have nearly total discretion to install monitoring software to protect their systems, the Justice Department fears that the use of such software at the direction of criminal investigators will lead to legal problems later. The victim of the attack and its system administrator may find themselves deemed to be agents of law enforcement if they cooperate too enthusiastically with the FBI and Justice. This is yet another example of a problem we encountered over and over; while law enforcement authorities provide a quick basis for gathering information about network attacks, they often bring with them so much encrusted criminal law doctrine that in the end the use of law enforcement authorities may not be worthwhile. We discuss later in the report some methods of addressing this problem, including the use of a civil remedy that avoids the need to bring in criminal authorities.)

indicted for everything examined in the investigation. In this vein, keeping grand jury proceedings secret prevents the release of derogatory information that ultimately was insufficient to persuade the grand jury to charge a crime. In this context, of course, it is *public release* of the information that is most important to prevent – the information is not kept from investigators, prosecutors, or the grand jurors. Thus, as a matter of policy, this vital privacy interest would seem to be best protected by making sure that any officials who have access to the information are subject to a confidentiality requirement.

It is not clear that barring dissemination of grand jury information to DoD personnel – who may already be subject to more stringent confidentiality disciplines than Rule 6(e) – adds much in the way of privacy protection for those under investigation. This is particularly the case today, when practically any harm to U.S. vital national security interests can also be investigated as a crime. In such investigations, the national security and criminal processes are already intimately coordinated. As a result, the national security agencies know quite well who is being investigated for, say, a major terrorist incident, and they already know what information the criminal investigators hope to obtain from the criminal process. In those circumstances, the suspects' privacy interest in preventing DoD from knowing that they are suspects is already fatally compromised. The case for withholding grand jury information from DoD on privacy grounds in cases where national security is at stake thus seems questionable at best.

Of course, prosecutors have their own reasons for defending the principle of grand jury secrecy, one that has nothing to do with the privacy of the suspect. Grand jury secrecy rules allow prosecutors to keep an investigation secret from the defendant, thus reducing risk of flight, intimidation of witnesses, and premature disclosure. While the commitment of prosecutors to keeping their plans secret is praiseworthy, in the task force's view this commitment must be balanced against the security needs of the nation. Prosecutorial secrecy cannot be absolute, and Rule 6(e) should not be read to protect it absolutely. Again, in almost every case of national security concern, such as terrorism investigations, criminal investigators are likely to reveal all facets of their investigations to the national security agencies and personnel involved in the investigations. Law enforcement already expects national security personnel to protect investigators' secrets as intensely as they protect classified information, with generally good success. Given all that, there is no obvious policy reason why the fruits of one particular investigative technique – grand jury subpoenas – should be kept from DoD to protect the prosecutors' interest in confidentiality.

A. Dissemination of grand jury information to DoD should be permitted

Given the weakness of the policy reasons for not sharing grand jury information, and the vital importance of allowing DoD access to information with a bearing on national security, the Justice Department should have taken a broad view of the dissemination authority already provided in Rule 6(e). As mentioned above, the rule allows dissemination to "such government personnel ... as are deemed necessary by an attorney for the government to assist an attorney for the government in the performance of such attorney's duty to enforce federal criminal law". (See Rule 6(e)(3)(A) and (C).) If the "duty to enforce federal criminal law" includes preventing or deterring assaults on networks of national security concern, sharing 6(e) information with DoD for that purpose is completely permissible. Since the rule also seems to leave the final decision to the attorney for the government and what he or she has "deemed necessary," one would have thought that a broad interpretation was eminently sustainable. After all, courts have allowed

prosecutors to share 6(e) information with state bar grievance committees, judicial councils investigating a judge's misconduct, and congressional committees considering impeachment. It is not unreasonable to conclude that protecting DoD networks from what may be state-sponsored attacks would be at least as important to the enforcement of federal law as disciplining private members of the bar.

In 1997, however, the Office of Legal Counsel once again adopted a position that does little to accommodate the concerns of national security bodies. Despite the sweeping language of the National Security Act, which commands all federal agencies to provide all intelligence-related information to the Director of Central Intelligence, OLC gives conclusive weight to one line from a 1983 Supreme Court decision, *Illinois v. Abbot & Associates, Inc.* In that case, the court refused to give state attorneys general access to federal grand jury testimony despite a federal law requiring the Attorney General to disclose information to state authorities in joint antitrust enforcement matters. In that context, the court declared that "we will not infer that Congress has exercised [its power to override grand jury secrecy] without affirmatively expressing its intent to do so." (See *Illinois v. Abbot & Associates, Inc.*, 460 U.S. 557, 572-73 (1983))

In the light of the Supreme Court's language, OLC's reasoning here is more justifiable than its opinion on Title III, but it is still highly questionable. One may reasonably doubt that the Court would have applied the same reasoning in the context of legislation on national security – a field where Congress speaks only rarely and then in the most general terms. But OLC saw no reason to hesitate; it applied the Court's language without regard for context. This application would be moderately persuasive if OLC had been willing to accept the logical consequences of its position. But OLC faced the obvious risk that such a strict rule would lead to disaster in the real world – where criminal and national security concerns overlap ever more often. What would happen, OLC was asked, if grand jury testimony uncovered vital matters of national security that then could not be disclosed to intelligence authorities (e.g., a plot to bomb an allied government facility abroad)? In the face of this concern, OLC faltered. If such information was uncovered, OLC declared, the President would have "inherent" authority to receive and order the sharing of information covered by Rule 6(e). This of course is the only responsible answer. But if the President has that authority, it is unconvincing to suggest that the President did not exercise it when he issued Executive Order 12333, which already requires all agencies to share intelligence information of any kind with the Director of Central Intelligence.

In short, the 1997 opinion is internally inconsistent and deserves reconsideration in the context of a broader agreement on information sharing about network attacks.

B. Materials obtained by grand jury subpoena should be shared with DoD.

The restriction on sharing grand jury information raises a second question: what is the scope of this restriction? Clearly, testimony given before a grand jury is a "matter occurring before the grand jury." If that were the full scope of the Rule, it probably would not be worth discussion here; such testimony rarely figures in investigations of the sort that NIPC conducts. (Moreover, if the same statements are made in the grand jury and in interviews to agents prior to grand jury testimony, as is often the case, the interview notes can almost always be divulged without running afoul of Rule 6(e).)

The problem is that Rule 6(e) can be read as extending not simply to testimony, but to documents and other information obtained by means of a grand jury subpoena. If Rule 6(e) is

read as barring DoD access to such information, it will impose significant barriers to prompt and easy sharing of information about network attacks with national security significance.

This task force is not in a position to canvass all of the case law about how Rule 6(e) might apply to subpoenaed materials, except to note that there is some divergence in the courts on this point. Prosecutors have successfully argued in some cases that disclosure of subpoenaed materials might disclose the direction of the grand jury's inquiries.⁹ Given this tactical value to prosecutors of grand jury secrecy, it is understandable that the FBI and Justice Department have reason to give Rule 6(e) a broad scope. Even so, there is reason for concern that NIPC's information-sharing protocol goes well beyond the requirement of Rule 6(e). For example, it expressly states, "For purposes of this Protocol, Grand Jury information also includes any material obtained pursuant to a grand jury subpoena." It is not limited to testimony or even to materials that would disclose the grand jury's lines of inquiry.

Whatever the reasons, it is difficult to see why the FBI or Justice should insist on this broad interpretation in the context of sharing information with DoD. Privacy concerns are particularly limited in this context. First, confidentiality agreements can be used to prevent DoD personnel from publicly releasing data in question. Second, whether subpoenaed information is protected by Rule 6(e) is often a matter of mere chance. Information identical to that obtained through a grand jury subpoena may usually be obtained by means of other criminal process that is not subject to Rule 6(e) – grand jury subpoenas are often used simply because they are faster or simpler to obtain than court-ordered discovery. Privacy is tenuous at best when it depends on the form that an investigator happens to fill out in the course of gathering evidence. And information should not be withheld from national security agencies simply because law enforcement used the path of least resistance to obtain it.

C. Investigators' use of grand jury subpoenas should be more effectively disciplined.

If it proves impossible either to limit Rule 6(e) to grand jury testimony or to give full effect to the executive order already requiring intelligence sharing, the difficulties arising from Rule 6(e) can still be minimized. Justice and the FBI could take internal action to greatly reduce the impact of Rule 6(e) on NIPC's ability to share information.

While it is legally necessary for the government to use some form of criminal process to obtain subscriber information from Internet Service Providers, investigators often have a choice of methods. They can obtain the information through grand jury subpoena or through an order under 18 U.S.C. § 2703(d). Information gathered under section 2703(d) is not subject to Rule 6(e) or its restrictions. The practical problem is that grand jury subpoenas are easier and faster to obtain – prosecutors need only show that the information sought is relevant to a criminal investigation. In contrast, obtaining a court order under section 2703(d), which would make a broader range of information available to investigators than that released pursuant to a subpoena, requires that the prosecutor state specific and articulable facts showing that evidence relating to a crime will be obtained, and present the proposed order to a judge.

A prosecutor or investigator in a hurry is likely to use a grand jury subpoena without worrying much about the problems it will later cause to other agencies in need of the

⁹ Again, it is worth noting that this consideration is of doubtful weight in a context where investigators' non-grand-jury inquiries are already thoroughly coordinated with national security agencies.

information. Current Justice Department policy encourages prosecutors to consider alternatives to grand jury subpoenas, but it is not clear that this suggestion is enforced by more than suasion. NIPC and Justice should establish rules prohibiting investigators and prosecutors from using grand jury subpoenas in investigating network attacks unless no other form of process will be as effective. Furthermore, investigators and prosecutors who persist in the use of grand jury subpoenas should be disciplined. The task force recognizes that sometimes speed is essential, and a grand jury subpoena is the fastest option. In that event, a second form of process should also be used to obtain the information in shareable form.

D. Legislative and executive solutions should be explored.

In the absence of (or in addition to) any other action, the position taken by OLC on sharing of grand jury information with DoD could be corrected, either by Congress or by executive order. Congress could make it clear that the National Security Act does indeed allow sharing of grand jury information with national security authorities. And the President could make it clear that Executive Order 12333 is intended to have the same effect. (In the context of national security, where the executive's authority is great, an executive order expressly requiring the sharing of Rule 6(e) information would very likely meet the "express statement" requirement set by the Supreme Court in *Illinois v. Abbot*.)

Before turning to the next recommendation, it should be noted that Justice and NIPC both take the view that Rule 6(e) has not often been a serious obstacle to information sharing in the context of network attacks. The task force agrees that a properly administered interpretation of Rule 6(e) should resolve most of the concerns. At the same time, no one asserts that Rule 6(e) never has or never will cause difficulties in the context of national security or network attacks. Moreover, Rule 6(e) is one of the obstacles to information sharing that is invariably raised by law enforcement as an essentially unsolvable legal problem. Coincidentally, this "unsolvable" problem also prevents complete openness with non-law-enforcement personnel, and ultimately forces a sharp distinction between the groups. In the task force's view, this insistence on separate regimes is itself likely to be a source of continued conflict and inefficiency. Every effort should be made to reduce or eliminate legal and cultural barriers to a seamless interaction of DoD and law enforcement personnel in the area of critical infrastructure protection.

RECOMMENDATION 1.5:

NIPC should report directly to the Director of the FBI and the Deputy Attorney General.

NIPC is – or could be – a vitally important interagency office. Assuming it can overcome the information-restricting policies criticized above, it has a large role to play in identifying and helping to respond to critical infrastructure attacks.

At present, however, NIPC is buried deep under a heavy FBI bureaucratic structure. It must pass through several levels of review before it can reach a Presidential appointee of any kind. This of course has unfortunate consequences for the office itself, but the concern is for the interagency process. It simply is not credible for the head of NIPC to perform an interagency coordinating function if his decisions must clear through three or four levels of FBI review before they reach the Director (let alone the Justice Department). Other agencies with flatter hierarchies will be discouraged from participating in NIPC's interagency coordination process if

the decisions reached in that process are subject to reconsideration at the insistence of mid-level FBI officials.

Indeed, some of the information-sharing disputes described to us festered longer than necessary because there was no ready way to escalate and resolve the issue at a level where some perspective could be achieved.

The task force recognizes that offices the size of NIPC rarely report directly to the Director of the FBI. For administrative and budgetary purposes, it may make sense for NIPC to be subsumed into a larger whole. But for policy and interagency matters, it should have a direct line, at least to the Director. Because resort to a political appointee may often be necessary to resolve interagency disputes, the task force also believes that NIPC should have direct access to the Deputy Attorney General.

RECOMMENDATION 1.6:

As part of a satisfactory framework agreement, DoD should upgrade its contribution to NIPC.

Although DoD's contribution to NIPC staffing is the largest outside the FBI itself, DoD has not sent as many detailees as it could, nor has it taken all possible steps to make a detail to NIPC as attractive as possible. In part, this may reflect doubts about whether detailees will be able to provide value to DoD while serving at NIPC. Assuming that problem is solved satisfactorily, DoD should take action to make sure that it sends a larger contingent of experts and properly supports them while on detail.

In general, this means that tours at NIPC should be two years, something toward which DoD now strives with only partial success. In addition, DoD should strongly consider making service at NIPC a "joint" assignment of the sort necessary for promotion to the higher ranks of the armed services. This would increase its attractiveness as a posting for military officers, and would help to ensure that NIPC is staffed with the highest quality detailees possible.

RECOMMENDATION 1.7:

DoD should clarify the role of NIPC in deciding how to respond to intrusions into DoD networks.

Any institution faced with a hacker, especially a persistent and successful hacker, has to make difficult judgments about whether to give top priority to blocking the attack or to observing the attacker's *modus operandi* in the hope of learning enough to identify or neutralize him. Locking the attacker out stops the immediate hemorrhage, but it may simply teach the hacker to switch to tactics that are less visible to the defenders, making the situation worse rather than better. Additionally, blocking out the hacker eliminates virtually any possibility of identifying the attacker and ascertaining his motives. But watching and waiting means that the hacker will continue to exploit the system.

The question for the government is: who should make the decision as to whether an attack should be blocked or watched? Within DoD the "block v. watch" decision is supposed to be in

the hands of the commander whose system is attacked. If more than one commander has information on the systems being attacked, the decision is evidently made by the Joint Task Force – Computer Network Defense (JTF-CND). At least one DoD element has made the decision to deploy tools that could tip off attackers, despite concerns expressed by law enforcement and perhaps other DoD elements about the “noisiness” of such tools. In the course of the debate over how to respond in that case, at least some DoD officials felt that NIPC and Justice were asserting the authority to influence the final decision. NIPC and Justice both deny any intent to assert such authority. Whether or not they did, the fact that neither should make this decision should be clarified in any agreement over NIPC’s role in critical infrastructure decision making.

At the same time, assigning responsibility for the decision is not the same as concluding that other agencies have nothing to offer the decision maker. NIPC has established a process for addressing “block v. watch” decisions. NIPC’s structure calls for a “senior group” review at which all interested agencies are represented. The senior group is a consensus body. Although NIPC may convene meetings, the head of NIPC is not supposed to have any more authority than any other participant. The senior group review process apparently has been useful in some circumstances, producing consensus decisions about how to handle sensitive investigations.

There are nonetheless some difficulties with this structure. It is not part of any formal understanding with any of the agencies involved. Thus, in the absence of a clearly defined decision path, it would be easy for people to believe that NIPC had assumed unilateral authority over a particular decision. In addition, it is difficult for NIPC’s interagency process to truly be a “senior” group when NIPC cannot speak for Justice or the FBI without clearing several internal levels of review.

There needs to be more clarity about the role of NIPC and the senior group in providing advice and making decisions about network attacks, including the “block v. watch” decision.¹⁰ Neither this task force nor NIPC finds fault with the current DoD rule that this decision lies with the commander whose system has been attacked. This allocation of responsibility should be recognized in the agreement between DoD and NIPC. It might also be dealt with by a broader interagency agreement or Presidential directive. But it is crucial that the authority to make the decision be clearly assigned, and recognized by all concerned parties.

RECOMMENDATION 1.8:

NIPC should not make independent judgments about what information intelligence agencies may and may not receive; in particular, it should no longer rely on its erroneous view of NSA’s authorities as a reason for restricting distributions to NSA’s information security organization. Additionally, neither NIPC nor the Justice Department’s Criminal Division should have any role in deciding how DoD entities should share information with NSA or other intelligence agencies.

The final area that should be clarified relates to information sharing with the National Security Agency (NSA). NSA has great resources and experience in this field. In addition to its

¹⁰ It is also important to note that, at least at the outset of an attack, it may be difficult to determine with any precision which systems are involved in the attack and whether the attack is state sponsored.

well-known intelligence-gathering mission, it has direct responsibility for the security of DoD information systems. Its experience and analytic capabilities on both the offensive and defensive sides make it a valuable participant in any effort to defend against network attacks. Depriving NSA of information about network attacks should therefore require substantial justification.

In actual practice, NIPC and Justice officials have shown considerable reluctance to give NSA information about network attacks, a reluctance that has often been justified by reference to legal concerns. But the need for clarification goes well beyond NIPC. In fact, even DoD itself has shown confusion about what information may lawfully be shared with NSA.

NIPC in particular frequently suggested that information sharing with NSA should be restricted to prevent an intelligence agency from gaining access to information about U.S. persons. There are two problems with this approach.

First, NIPC, the FBI, and indeed most of the Justice Department simply lack the expertise necessary to determine what limits apply to intelligence agencies' use of information. In general, intelligence agencies are barred from targeting Americans for surveillance, but they are not barred from reviewing information gathered elsewhere about Americans. (Any other rule would call into question the distribution of U.S. newspaper clips at intelligence agencies.) As a general rule, legal restrictions on intelligence agencies are grounded in the conviction that the fearsome capabilities of these agencies should not be aimed at U.S. citizens. But information in the hands of NIPC has not been gathered by intelligence agencies. Thus, allowing intelligence agencies to examine such information for analytic purposes does not point U.S. intelligence capabilities at American citizens.

Second, there is no reason to think that the usual intelligence oversight mechanisms are not functioning, or that NIPC or the Justice Department's computer crime experts should act as an intelligence oversight body. NIPC in particular should not seek to act as NSA's watchdog in a context where its actions might be construed as simply defending turf. In general, if there are questions about the lawfulness of intelligence agency access to particular information, NIPC's job should be limited to raising the issue with the relevant agency's general counsel, the Justice Department's Office of Intelligence Policy and Review, or both.

Along the same lines, the Justice Department's Criminal Division has encouraged a much-too-narrow view of when DoD may share with NSA information that it acquires in the course of administering security measures. The Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) has argued that a DoD systems administrator should not share information about attacks on DoD systems with intelligence agencies. This is a harsh limit, since it prevents NSA from analyzing hacker tactics even when the hackers are attacking DoD's own computers. The origins of this notion lie deep in Justice Department lore. But in the task force's view, that lore has little relevance in other contexts.

Broadly speaking, Title III and its progeny make all intercepts of electronic communications illegal in the absence of a statutory exemption. This creates a potential problem for network operators and systems administrators, who often are exposed to the contents of communications over their networks and who sometimes actively monitor those communications to protect against security breaches. To make sure that this activity was not outlawed, Congress provided that the agents of a service provider may monitor communications "while engaged in any activity which is a necessary incident to the ... protection of the rights and property of the provider." In

reliance on this provision, system administrators may record every keystroke a hacker makes while on their systems.

Sooner or later, instead of just watching the attacker, systems administrators may decide to call in the police. But unlike the systems administrator, the police may not simply record all of the communications of a criminal suspect, unless they have a court order. Faced with such a burden, the police are naturally tempted to ask the system administrator to continue monitoring for purposes of gathering evidence. To avoid this result, courts and the Justice Department have sought to prevent investigators from "tasking" service providers or otherwise turning systems administrators into agents of law enforcement.

At some point however, the Computer Crime and Intellectual Property Section came to believe that, if police and prosecutors could not work closely with systems administrators, then neither could intelligence agencies like NSA. The theory was that Title III only allowed monitoring of networks for security purposes, not for purposes of law enforcement or intelligence gathering.

There are two problems with this conclusion. First, it mischaracterizes NSA as simply an intelligence agency. While NSA does indeed gather signals intelligence, it also has another and quite separate mission – information security. This is carried out by a large office devoted entirely to providing information security for DoD. This office is not part of the intelligence community, it has no intelligence role, and for that reason it is not subject to the intelligence-targeting restrictions that apply to the intelligence side of NSA. In short, there is no reason to deny NSA's information security office access to information on the basis of intelligence agency limitations.¹¹

Second, there is reason to doubt the Justice Department's assumption that if the police and prosecutors may not work closely with systems administrators monitoring a hacker, then no one may. In fact, police and prosecutors are subject to strict, court-enforced rules about how they gather evidence against criminals, and any deviation from those rules is likely to draw careful scrutiny. Therefore, for reasons having to do with public policy and judicial oversight, prosecutors are not allowed to circumvent those restrictions by "laundering" their evidence-gathering through systems administrators.

This is the most reasonable reading of the system administrator exception to Title III. For many reasons, systems administrators need broad authority to conduct monitoring, and as long as that monitoring has a plausible relation to a security concern, their actions must be lawful. Any other rule would require systems administrators to walk a knife edge each day, with the constant threat of felony prosecution if their subjective motives were deemed to fall over the fine line between proper monitoring (for a security purpose) and improper monitoring (for some other purpose). If the monitoring has been performed lawfully, Title III gives systems administrators virtually unlimited authority (under Title III) to disclose the results of the monitoring.

¹¹ To be fair, DoD has not always been clear on this point either. For example, doubts have been expressed about whether DoD logs showing the tactics of intruders can be shared with NSA analysts, since the nationality of the intruders cannot be known, though in many cases they hack in from U.S. hosts. The answer appears clear enough. First, the information security side of NSA is part of the DoD computer security apparatus. Anything that a systems administrator can review for security purposes can be shared with NSA's information security office. Since it is clear that doubts on this point remain even within DoD, it should be made plain both inside the DoD and in any framework agreement with NIPC.

On that reading, there is little or no basis for the Justice Department to question the sharing of DoD system administrator logs with NSA – or other intelligence agencies for that matter. The ultimate goal of that sharing is better network security, and the role of the intelligence agencies in analyzing and circulating information about attacks is in many ways similar to that of the Computer Emergency Response Team (CERT), which also circulates intelligence gathered from systems administrators about attacks on their systems.¹²

RECOMMENDATION 2:

A Standardized and Simple Set of Procedures Should be Adopted to Allow Unannounced “Red Team” Attacks on All DoD Networks Without Excessive High-Level Intervention by DoD Lawyers.

The task force does not mean to leave the impression that all of the legal difficulties that have hindered DoD’s preparations for information attacks can be traced to NIPC, the FBI, or the Justice Department. Some have been home-grown.

The effectiveness of “red team” operations in uncovering vulnerabilities in government computer networks is undisputed. Indeed, these simulation attacks have done much to show just how unprepared the United States is to defend itself against a significant information warfare offensive. In the past, however, conducting a red team attack on a DoD element has required extensive internal approvals, climbing up both the tested and testing agency command structure, and culminating in DoD General Counsel and Secretary of Defense approval on a case-by-case basis. This was because DoD took a belt-and-suspenders approach to the legality of red team intrusions. To ensure that there were no legal questions about the red team’s right to gain access to DoD computer files, DoD sought assurances that all users had consented to red team access, which could only be determined after a review of each system. Since DoD users receive consent notices regularly both in hard copy and through system banners, this should not have been difficult to establish, but in the early days of the program, great care was taken to double- and triple-check the consents for each system and each exercise.

The task force believes that this degree of care is no longer necessary. The task force noted that DoD has made real strides lately in reducing the complexity of the red team approval process without any adverse consequences – and with real advantages in terms of security. The approval process is more streamlined, and red-teaming is no longer seriously constrained by determinations of consent. Nonetheless, the Secretary of Defense is still being asked to review individual red team exercises and certify consent. This is an unnecessary burden on the secretary and on the red-team process. Now that red-teaming is becoming a standard part of DoD security measures, the task force recommends that instead of reviewing individual exercises the Secretary simply certify periodically that DoD systems and users have consented to network monitoring.

¹² The fact that some of the information is circulated in classified form makes no difference; systems administrators themselves could choose to centralize corporate security information and circulate it to a limited number of trusted employees, and they could do so without worrying that gathering information for such purposes is somehow outside the scope of their legal authority.

RECOMMENDATION 3:

Specific Legislative Revisions Should Be Made to Facilitate Interagency Information Gathering and Sharing.

The proposals listed above focus on matters of agency policy and procedure that should be revised in order to facilitate more effective defensive information operations. The task force concentrated its attention on reforms that lie, at least in part, within the power of DoD. Of course, nothing would prevent Congress from acting to require a charter for NIPC, or from incorporating any or all of these recommendations for such a charter. But the task force sought to avoid issuing a report that was dependent on legislative action for its implementation.

Nonetheless, it became clear in the course of task force discussions that the current legal framework for defending against information warfare is flawed in several ways that only Congress can cure. The task force did not proceed from the assumption that this framework requires a complete overhaul. Quite the contrary, we resisted recommendations for legislative action whenever we thought the problem could be resolved by a more reasonable administrative interpretation. Despite this resistance, the task force became convinced that some changes in existing law are appropriate if a unified and effective response to information warfare is to be mounted. The task force's proposals for a legislative agenda in this field are contained below.

RECOMMENDATION 3.1:

DoD should have the authority to seek information about network attacks through a civil investigative order, specifically to combat attacks on systems of national concern.

Time and again, efforts to streamline information sharing have struggled with the structure of rules that has grown up around the class of information that is gathered in a criminal investigation. So long as information about attacks is gathered primarily through criminal investigative methods, that information will carry with it a set of legal and cultural rules that are hostile to the sharing needed to respond effectively to network attacks.

Perhaps the most egregious example of forcing all information gathering into a criminal law straitjacket is 18 U.S.C. § 2703(c). This provision of law limits the circumstances in which a service provider may disclose information about customers or subscribers to a governmental entity. For basic subscriber information (name, address and the like), the government must produce an administrative, grand jury, or trial subpoena. For more detailed "transactional" data about customers, the government must: (1) present a search warrant under the Federal Rules of Criminal Procedure or equivalent state warrant, (2) obtain a criminal investigative order under § 2703(d), (3) have the consent of the subscriber or customer, or (4) submit a formal written request for name, address, and place of business when relevant to a law enforcement investigation of a telemarketer. *See* 18 U.S.C. 2703(c)(1)(C).¹³

Even the most minimally competent cyber attacker uses multiple "hops" between computers to launch attacks. This permits the attacker to cover his or her tracks much more effectively. In consequence, tracking hackers requires a series of investigations, essentially tracking backward from one host computer to another. Typically, authorities will be able to use a victim's own logs

¹³ Subparagraph (D) of the same section allows the gathering of certain information about subscribers using administrative, grand jury, and trial subpoenas. None of these subpoenas is suitable for most DoD inquiries, since one is criminal, another requires that a trial be imminent, and the third requires some administrative authority that is not obviously granted to DoD.

to identify the initial source of an attack; they then contact the system administrator for the computer that is the source of the attack, ask for access to the logs of that host, and try to determine who was logged onto the computer at the time of the attack so as to determine the second "leg" of the hacker's travels. Once the second leg has been identified, the process is repeated, often many times. At every stage in this process, section 2703(c) limits the information that can be provided to government agencies.

It is worth noting that the restriction imposed by section 2703(c) applies only to requests for information made by government agencies. Internet service providers (ISPs) may hand out subscriber information on street corners to all comers without violating any provision of law; they may sell subscriber information to pornography spammers without violating any provision of law. (As a practical matter, of course, most ISPs have instituted privacy policies that voluntarily restrict distribution of customer data.) More realistically, they may share information about network attacks with other ISPs and hosts on a real-time basis without having to stop and invoke the judicial process at all. But they will violate the law if they provide information to a defense agency – even in the midst of a serious attack – without first seeing a criminal investigative order.

This is a remarkable state of affairs, and not one intended by the drafters of section 2703(c), or so one would hope. In general, if a government site is attacked and seeks information about the source of the attack from the first "hop" in the chain, the ISP with that information runs a slight risk that section 2703(c) will be violated if he simply tells the government what he knows about the intruder. That is because at this stage no one knows who the hacker is. He could be a subscriber or customer of the ISP. Chances are that he isn't, but why should the ISP risk civil liability? The prudent thing is to demand a criminal investigative order. Thus, in the name of protecting customers and subscribers, the current law actually puts a significant barrier in the way of protecting those who use government systems.

What's more, the provision essentially forces the government to treat all intrusions that require investigation as criminal matters. This serves no one's interests. If the culprit is a juvenile, prosecution is unsatisfying for the government and damaging for the defendant. Both might be better off if, instead of always relying on criminal investigations, the government could also gather necessary information while pursuing only civil remedies, such as fines, compensatory payments, or tailored injunctive relief. Indeed, some of the most important hacking investigations have not produced significant criminal penalties – at least not in the United States. (One investigation that consumed vast amounts of government resources finally tracked the exploits to two California teenagers and a young Israeli. No significant criminal penalties were imposed in the United States, and the Israeli proceedings have not yet produced a final result. Similarly, a 15-year old boy in Canada is the only person arrested thus far in the celebrated denial-of-service attacks in early 2000. The perpetrators of the "ILOVEYOU" virus will not be prosecuted in the United States.)

Allowing civil discovery in these circumstances is an option that deserves consideration. It is not without risks: ISPs and portals will not welcome any expansion of electronic communications discovery. At the same time, for DoD, there are advantages to information gained in a civil action. First, of course, it can be shared much more readily among agencies and through NIPC. It is not subject to grand jury secrecy concerns, nor to the Justice Department's restrictions on sharing information with NSC, nor is it likely to be "law enforcement sensitive." Indeed, since it would be gathered by DoD, it could be shared freely without even the restraints

imposed by FBI culture on NIPC. This factor becomes extremely important when the target of an attack is a computer or network that is crucial to civil and national defense.

Second, being able to move from a purely internal defensive response to a civil investigative response will resolve another problem that has dogged DoD system administrators from the beginning of their work with Justice. This is the "prosecutorial agent" problem discussed above. In general, systems administrators may monitor as closely as they like those who intrude into their networks, without any legal prerequisites. DoD security officials have taken advantage of this fact, but they have complained that bringing criminal investigators into the matter often complicates their efforts to monitor an attacker. This is for the reasons described above – criminal investigators are acutely aware that they must have independent legal authority for intercepts and cannot turn a systems administrator into an agent of law enforcement. This is less of a risk if systems administrators are gathering information for a civil action.¹⁴ Thus, network security officers could move from purely defensive monitoring to a civil investigation, including requests for information from third parties, without ever running the risk that a court would treat those actions as showing that the investigation is "really" a criminal investigation.

There are some drawbacks to the use of civil investigative authority. First, gathering data for the purposes of a civil investigation is complicated if, as with network attacks, there is a possibility of criminal prosecution. Second, DoD would need an appropriate civil discovery authority. And without some incentive to the ISP in question (such as an offer by DoD to pay the cost of expedited processing), the civil process could be significantly slower than a criminal one. Finally, many ISPs have instituted policies to provide notice to customers when law enforcement officials request data pertaining to them, a practice that effectively eliminates the secrecy of an investigation. Still, these are all issues that could be ironed out legislatively for the sake of protecting a nationally sensitive computer system.

A final issue that will undoubtedly be raised in this context concerns privacy. Should DoD be able to obtain subscriber information in network attack investigations without meeting the requirements for a criminal investigation? One may begin by asking whether investigating attacks on national security networks are as important as investigating telemarketers, since Congress has already exempted telemarketing investigations from the criminal subpoena requirements. What's more, a civil discovery authority limited to network attacks would not expose hackers to any greater risk of investigation than they now face; almost all network attacks can be investigated as crimes using criminal process. If necessary, Congress could require precisely the same standard for the civil discovery order as for a criminal order. If so, only two things would be different. First, the government would not be required to begin every investigation as though it was destined to end in indictment, and the authorities would be able to shape their legal response more sensitively in the light of the intruder's age, motives, and status. Second, the information would be gathered directly by DoD rather than the FBI and Justice. Whether that raises privacy concerns depends on which agency is considered more of a privacy threat. Certainly, there is no reason to think that DoD should be barred as a matter of principle from discovery aimed at civilians; defense investigators already serve a variety of civil processes on DoD employees and contractors, as well as ordinary discovery orders in garden-variety civil

¹⁴ No one thinks that private companies may not lawfully ask their system administrators to gather information about hacker intrusions that they intend to use to sue the hackers. If there are real fears that current law somehow prevents the government from following this example, the statute authorizing the civil suit could no doubt also authorize the use of such information in support of the suit and for other network defense purposes.

litigation. Properly structured, a civil discovery authority for network attacks would pose no greater threat to civilian privacy than the government's existing powers.

Network security would be greatly advanced, and the privacy status quo would be preserved, by a legislative provision overriding section 2703(c) and permitting the collection of data under a civil investigative order when the target of attack is a system of national security importance.

RECOMMENDATION 3.2:

The gap between law enforcement and foreign intelligence authorities to intercept hacker attacks should be closed, by enacting a "network trespasser" exception to Title III or otherwise.

Another somewhat surprising limitation on the ability of the FBI to gather information under criminal authorities has emerged of late. Under the Foreign Intelligence Surveillance Act (FISA), once a factual predicate has been established – that the target of an investigation is an agent of a foreign power – intercepts may be maintained for relatively long periods of time.¹⁵ A Title III intercept, however, must be renewed every thirty days, with the Justice Department obligated to persuade the presiding judge that the tap is crucial to an ongoing criminal investigation.

But hacking investigations may take years without bringing investigators significantly closer to actually indicting a particular human being. Continuing the intercepts may be crucial to gathering information about the techniques used by the hacker and gathering clues about the hacker's identity and motives, but the process can be a slow one.

Sometimes a Title III intercept shows that the hacker is probably based abroad, and in such cases, over time, a criminal investigation will begin to appear futile. Hacking may not be a crime in the suspected country of origin, or the hacker may not be extraditable, or it may be impossible to get the cooperation of the local police. Gradually, the intercept begins to have less and less value as a criminal investigative tool, even though maintaining the tap may be highly important from an intelligence point of view. Sooner or later, then, prosecutors (at least the prosecutors in the Computer Crime and Intellectual Property Section (CCIPS) which is the source of this concern) are likely to reach the conclusion that the legal standard for continuing the wiretap is no longer satisfied. At that point, the prosecutors will refuse to seek additional wiretap authority – even though a criminal intrusion is still occurring, and even though the evidence may suggest that the intrusion is sophisticated enough to be state sponsored. The CCIPS view is that Title III is not an intelligence-gathering authority; unless a criminal case is in the offing, the tap must end, notwithstanding the value of the intelligence to national security. Of course, if it is clear that a foreign government is involved, a foreign counterintelligence tap can be initiated, but this is rarely clear. The result is that important intelligence about network attacks will be lost. In short, there is a very real possibility that foreign hackers will be able to attack DoD systems without any wiretap monitoring because both existing law enforcement and counterintelligence authorities are too narrow.

¹⁵ FISA permits the surveillance of the agent of a foreign power under a court order, which must be renewed every ninety days. The foreign power itself may be targeted for an entire year under a court order pertaining to FISA.

For this and other reasons (e.g., statutory information-sharing restrictions), Title III intercepts are an unappealing way to gather information about hacking efforts. That said, it is unclear what alternatives exist unless Congress addresses the problem. In that regard, two approaches should be considered.

First, the Justice Department, or at least CCIPS, would welcome DoD support for a "trespasser" exception to the protections of Title III. In essence, this would deny any statutory expectation of privacy to persons who are trespassing on another person's computer network. This is indeed an appealing approach, as hackers should not have any expectation that the signals they send to the systems of victims will be free from monitoring. This proposal has circulated within the Justice Department but has not been advanced officially. DoD should support such a measure.

A second possibility is to seek amendments to FISA that would allow the courts to presume that a foreign power is involved when attackers hop through hostile countries, attack critical systems, and/or use techniques that are thought to be particularly sophisticated or otherwise characteristic of foreign powers. There is some room for making this argument in the context of existing law, but it would obviously be easier if such considerations were part of FISA.

In so saying, the task force does not underestimate the difficulties of such a modification. The nation will not – and should not – tolerate long-term intelligence surveillance of Americans; no one wants to authorize FISA intercepts that turn out to be aimed at the activities of California teenagers. While it is likely that that result can be avoided if sufficient care is exercised in defining the events that justify such surveillance, any such amendment to FISA would need to be carefully drafted, vetted, and debated. Before making a change, it would be appropriate to ask (as task force members could not, being limited to a secret clearance) whether it is possible to utilize overseas intelligence collection resources to gather information on the attack, thus avoiding the need to invoke FISA at all. Intelligence collection efforts outside of the United States face fewer restrictions on gathering information relating to attacks than do domestic law enforcement investigations. For a variety of reasons, the task force thinks it unlikely that this is a complete answer, but it should be examined with care by DoD before making a final decision on the kinds of legislative changes that are appropriate to address the pressing problems that have been identified above.

RECOMMENDATION 3.3:

Procedural improvements should be made to streamline the "trap-and-trace" process and to allow emergency data requests under Electronic Communications Privacy Act (ECPA).

A. Trap-and-trace improvements.

When a network attack is being investigated, it is normal to obtain, first, a § 2703(d) order for information already in the hands of the first ISP in the chain of attacks, and, second, a trap-and-trace order authorizing future information collection for law enforcement purposes.

The use of trap-and-trace orders, however, has not been free from difficulty. Trap-and-trace orders are ordinarily obtained in the jurisdiction where the trap-and-trace device is to be placed (i.e., in the jurisdiction of the service provider). Since the Internet has little interest in

geography, it is typically the case that every leg of a hacker's journey terminates in a different city, and with a different service provider. Often these providers are located in different jurisdictions, and obtaining the requisite orders can cause delays. Delay is the enemy of any investigation, but particularly of hacking investigations, as hackers often change their patterns regularly, sometimes as frequently as every few hours or minutes.

Delays in obtaining trap-and-trace orders for facilities in particular jurisdictions disrupt the ability of investigators to trace back along a hacker's attack chain. In particular, if there is a live connection, tracing back an attack quickly is difficult because each step in the chain may require a new order (because the carriers may be in different jurisdictions), each based upon the information discovered in prior orders. Moreover, the review by multiple courts does not substantively protect any rights, since the court in the victim's jurisdiction has already determined the appropriateness of the trace, and other courts are merely effectuating the order of the first court. Timing is also critical where the investigation concerns an attack that has already taken place, as the investigating agency must obtain a court order to trace the attack through activity logs before the service providers whose networks are used in the attack overwrite their records.

In response to this concern, investigators have expressed interest in obtaining a single national trap-and-trace order that could be served progressively on each service provider who has been the inadvertent host of a hacker on his journey.

In general, such authority would reduce the time it takes to track hackers, though there are many reasons for delays in tracking hackers from one computer to the next. Obtaining trap-and-trace orders is a contributor to those delays, but it is not the only contributor. For example, even with a nationwide order, it will still be necessary for the authorities to go from provider to provider in an aching sequential fashion. This "one step at a time" approach is an unquestionable source delay in some hacking investigations.

Given these limitations, a nationwide trap-and-trace authority is not a panacea. But it would have some value to Justice and DoD in seeking to find network attackers as quickly as possible. For that reason, it deserves support – so long as that support does not detract from the other, higher priority, legislative reforms set forth earlier.

B. Emergency authority under ECPA.

A second revision also deserves consideration. Currently, there is no statutory provision for government to obtain information quickly under the ECPA in situations of extreme urgency. This is an oddity, since wiretaps, presumably much more intrusive, may be initiated without a judicial order in "emergency situations."¹⁶ In such cases, where a communication must be intercepted "before an order authorizing such interception can, with due diligence, be obtained" (and where there are sufficient grounds to assume that an order would ultimately be granted), an intercept may be conducted in absence of authorization, provided that approval of the intercept is requested within forty-eight hours after "the interception has occurred, or begins to occur." (See 18 U.S.C. § 2518 (7))

¹⁶ Emergencies are defined as involving:

- (i) immediate danger of death or serious physical injury to any person;
- (ii) conspiratorial activities threatening the national security interest; or
- (iii) conspiratorial activities characteristic of organized crime

The information that can be obtained through a subpoena or section 2703(d) order is sometimes equally essential to the investigation of a hacker attack, and providing specifically for emergencies would be useful. It would also protect the interests of ISPs and those under investigation. As things now stand, the lack of a statutory emergency provision means that in an emergency law enforcement agencies put heavy pressure on ISPs to release information even before the authorities can produce an order. The release of this information (which almost always happens) can expose the ISP to liability for violation of its privacy policy, and can cause law enforcement authorities to come to rely on the emergency justification (even in cases where the emergency isn't all that clear). In the long run, as customer privacy becomes the subject of greater scrutiny in state and federal legislatures, ISPs may discontinue their current practice and refuse to release any information in the absence of an order. The current provision in Title III allowing emergency wiretaps should be extended to court orders and subpoenas as well.

RECOMMENDATION 3.4:

Federal Rule of Criminal Procedure 6(e) should be modified to allow sharing of grand jury information relating to national security.

The task force has already discussed (see **Recommendations 1.3 and 1.4**) information-sharing burdens that are created by the use of grand jury subpoenas or Title III intercepts to gather information about network attacks. The task force recommended several ways in which these problems could be solved through reasonable accommodations of the national security by Justice and NIPC. In the event that these agencies are not prepared to make those accommodations, it may be necessary to overcome these obstacles legislatively. No one believes that either Title III or Rule 6(e) was written deliberately to exclude sharing for national security purposes. Very likely, it simply did not occur to the drafters to include a national security provision. Curing this oversight legislatively, perhaps simply by clarifying the existing National Security Act, ought to be a live option.

RECOMMENDATION 3.5:

Legislation should be enacted to encourage voluntary private-sector cooperation in hacking investigations, specifically to quell concerns that sensitive or proprietary information might be disclosed publicly.

Much has been made above of the legal barriers that prevent the government's access to or sharing of information when conducting hacking investigations. These are by far the most significant obstacles to efficient defensive information operations. They are not the only barriers, however, as even information that investigators could lawfully acquire is sometimes kept out of reach.

The investigation of cyber attacks need not be a one-way event, with law enforcement issuing various orders for information and service providers consequently handing it over. An ISP that falls victim to a hacker attack may justifiably hand over information about the attack, at the very least to prove that a crime has taken place. All too often, however, the private sector resists such voluntary cooperation with law enforcement. There are a number of reasons for this

reluctance, most notably a fear that the information shared may be released under the Freedom of Information Act (FOIA).

So much of the nation's critical infrastructure is based in private hands that the importance of that sector's voluntary cooperation in investigations on network attacks should not be underestimated. This being the case, the government should adopt reasonable measures to encourage this cooperation. Agencies should be encouraged to expand the use of nondisclosure agreements in gathering information on network attacks. In addition, it would be worthwhile to consider supporting legislation that would restrict from FOIA disclosure any information that a service provider shares in conjunction with a hacking investigation (legislation to this effect was introduced in the last Congress and will likely be reintroduced). Such legislation should be narrowly tailored, so as to avoid creating an exemption behind which companies could conceal evidence of unlawful business practices from public discovery. Even with these limits, the provision could have significant benefits for investigators of network attacks.

APPENDIX A. ACRONYMS

CCIPS	Computer Crime and Intellectual Property Section
DAG	Deputy Attorney General
ECPA	Electronic Communications Privacy Act
FISA	Foreign Intelligence Surveillance Act
FOIA	Freedom of Information Act
ISPs	Internet service providers
JTF-CND	Joint Task Force – Computer Network Defense
MOU	Memorandum of Understanding
NIPC	National Infrastructure Protection Center
NSA	National Security Agency
NSC	National Security Council
OLC	Office of Legal Counsel
ORCON	Originator Controlled

APPENDIX B. PANEL MEMBERS AND GOVERNMENT ADVISORS

Chairman:

Mr. Stewart Baker	Steptoe & Johnson
-------------------	-------------------

Members:

Ms. Elizabeth Banker	Yahoo! Inc.
----------------------	-------------

Mr. Bill Burrington	AOL Europe
---------------------	------------

Mr. Roger Callahan	Bank Of America
--------------------	-----------------

Mr. Scott Charney	Pricewater-HouseCoopers LLP
-------------------	-----------------------------

Mr. Steven DeGeorge	AT&T Law Division
---------------------	-------------------

Mr. Lawrence Greenberg	The Motley Fool, Inc.
------------------------	-----------------------

Mr. Jonathan Spear	MCI Telecommunications Corporation
--------------------	---------------------------------------

ANNEX F

1996 DSB Report on Defensive Information Operations

STATUS OF RECOMMENDATIONS

**Current Assessment of Recommendations from the
Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)**
(November 1996)

1996 Recommendation	Current Status	Current Shortfalls
1. Designate an accountable IW focal point. The SECDEF should:		
1a. Designate ASD(C3I) as the accountable focal point for all IW issues.	DoD Directive S-3600.1 "Information Operations," 9 Dec 96, designates ASD(C3I) as the responsible authority for IW/IO.	
1a(1). Develop a plan and associated budget beginning in FY97 to obtain the needed IW-D capability.	Components were required to address IA budgets beginning with FYDP 1999-2002. The DIAP was established by DEPSECDEF to better coordinate and align IA budgets and assure adequate funding. – this effort has provided better visibility for overall DoD IA budget.	<ul style="list-style-type: none"> • There are no specific line items for IA. • Shortfalls identified by DIAP have been faced with a shortage of additional funds.
1a(2). Authorize ASD(C3I) to issue IW instructions.	DoD Directive S-3600.1 "Information Operations," 9 Dec 96, designates ASD(C3I) as the responsible authority for IW/IO. In addition, the DoD implementation of the Clinger-Cohen Act designates the ASD(C3I) as the DoD CIO and assigns the responsibility for IA to the DoD CIO.	
1a(3). Consider establishing a USD(Information).	No longer required; the ASD(C3I) has been designated the DoD CIO.	
1b. Establish a DASD(IW) and supporting staff to bring together as many IW functions as possible.	The June 1998 reorganization within OASD(C3I) resulted in the creation of a DASD for Security & Information Operations, a position that includes responsibility for Information Assurance, Infrastructure Assurance, Security, Counterintelligence, and Information Operations Strategy and Integration.	This organizational structure resides within OASD(C3I) and primarily includes those activities currently within the purview of OASD(C3I). This structure does not readily accommodate the corresponding DIO-related requirements/issues within OUSD(A&T), including related R&D within DARPA and the Military Departments.

1996 Recommendation	Current Status	Current Shortfalls
2. Organize for IW-D.		
2a. Establish a center to provide strategic indications and warning, current intelligence, and threat assessments. The SECDEF should request the DCI to:	NSA established the National Security Incident Response Center (NSIRC).	This organization is primarily focused on tactical activities rather than strategic activities, although in some cases, tactical level incidents may yield strategic insights.
2a(1). Establish an I&W/TA center at NSA with CIA and DIA support.	The DIA and JWAC are involved in this area.	There appears to be no overall DoD orchestrated approach to providing a strategic capability for DIO.
2a(2). Task and resource the Intelligence Community to develop the processes for Current Intelligence, Indications and Warning, and Threat Assessments for IW-D.	There are numerous activities within the Intelligence Community to address the intelligence requirements.	It is unclear as to how well these various activities are coordinated.
2a(3). Encourage the Intelligence Community to develop information-age trade craft, staff with the right skills, and train for the information age.	The DCI established the Advanced Research and Development Technology activity under NSA to focus on information technology as a multidisciplinary capability to the Intelligence Community.	The available skill set continues to fall well below the need.
2a(4). Conduct comprehensive case studies of U.S. offensive programs and a former foreign program to identify potential indicators – collection, funding, training, etc.	The DTRA “Chessmaster” case study is an example of the type of activity currently ongoing. Assessments continue as the capabilities and intentions of potential opponents change.	
2a(5). Establish an organization to examine and analyze probable causes of <u>all</u> security breaches.	NSA established the Network Incident Analysis Cell (NIAC) within the NSIRC to perform post network intrusion, forensic-style analysis of data received from incident response centers.	Analytical results and lessons learned are not effectively disseminated.
2a(6). Develop and implement an integrated National Intelligence Exploitation Architecture to support the organization and processes.	Intelligence Community activities in this area are ongoing.	Efforts are disparate and not integrated into a well-described plan.
2a(7). The SECDEF should direct the development of IW Essential Elements of Information (EEI).	Intelligence Community activities in this area are ongoing and JTF-CND is providing input into development of EEIs.	No final product or publication date has been set.

1996 Recommendation	Current Status	Current Shortfalls
2b. Establish a center for IW-D operations to provide tactical warning, attack assessment, emergency response, and infrastructure restoration capabilities. The SECDEF should:	The DoD established the Joint Task Force - Computer Network Defense (JTF-CND) and the DISA Global Network Operations Center (GNOSC).	Concepts of Operations (CONOPS) for DIO mission execution are immature or do not exist. Where mission assignments have been made, lack of resources inhibits execution (e.g., USSPACECOM, JPO-STC).
2b(1). Establish a DoD IW-D operations center at DISA with NCS, NSA, and DIA support.	The DoD established the DISA Global Network Operations Center (GNOSC).	DoD does not universally collocate its Network Operations Centers with Information Assurance (IA) / Computer Network Defense (CND) activities.
2b(2). Develop and implement distributed tactical warning, attack assessment, emergency response, and infrastructure restoration procedures.	Currently, JTF-CND does distribute tactical warning, but has minimal attach assessment capability. Emergency response is primarily coordinated through the various CERTS/CIRTS of the Services / Agencies. JTF-CND also assists in establishment of restoration priorities with DISA and other activities.	Recommended improvements in GIG architecture and security could provide a technology baseline to permit creation of a tactical/time-sensitive information attack warning sensor grid. Such a network would also support goals of assigning attacker attribution confidently and rapidly. However, any plan to achieve this outcome must span the domains of policy/law, technology and organization, and would require actions in several sectors of government, as well as private industry.
2b(3). Interface the operations center with Service and Agency capabilities and I&W/TIA support.	This requirement is stated in the JTF-CND Concept of Operations; JTF-CND interfaces with these organizations continue to strengthen.	DoD CERT/CIRT activities vary in their execution and are not inclusive of all DoD CINCs/Services/Agencies.
2b(4). Establish necessary liaison (e.g., with military and government operations centers, service providers, intelligence agencies, and computer emergency response centers).	This requirement was completed as a result of the JTF-CND Concept of Operations.	
2c. The SECDEF should establish an IW-D planning and coordination center reporting to the ASD(C3I) with interfaces to the intelligence community, the Joint Staff, the law enforcement community, and the operations center.	The Defense-wide Information Assurance Program (DIAP) was established in 1998. It serves primarily as a facilitator for the gathering and sharing of IA-related information. In that role, the DIAP has accomplished much in identifying what is being done throughout DoD, and continues to focus on unifying/integrating various IW-D activities.	<ul style="list-style-type: none"> The DIAP has no real authority to direct the Military Departments or Agencies, and does not control or impact any IW-D aspects of Service/Agency budgets. Internal staffing and funding shortfalls have further hampered the DIAP's ability to accomplish the mission.

1996 Recommendation	Current Status	Current Shortfalls
2d. Establish a joint office for system, network and infrastructure design.	There are current activities to develop, promulgate and implement Joint Technical Architecture (JTA), Joint Operational Architecture (JOA) and Joint Systems Architecture (JSA). Many recent efforts have centered on development of GIG architecture.	<ul style="list-style-type: none"> There is no joint office to coordinate these various activities. The GIG IATF standards and protocols for providing security are inconsistent with the JTA.
2d(1). Establish a joint security architecture/design office within DISA to shape the design of the DoD information infrastructure.	OASD(C3I), DISA, NSA, Joint Staff and Service representatives participate in the activities cited in 2d.	<ul style="list-style-type: none"> There is no joint office to coordinate these various activities. The IATF is a collection of history and general information; it is not a document that can be used to implement interoperable, secured information systems for DoD.
2d(2). Establish a process to verify independently and enforce adherence to these design principles.	The DoD established the Defense Information Technology System Certification and Accreditation Process (DITSCAP), as well as the Secret And Below Interoperability (SABI) and Top Secret And Below Interoperability (TSABI) processes. Processes within the GIG governance arena are also being established to enforce adherence to GIG architecture requirements.	There are insufficient resources to implement DITSCAP, SABI, and TSABI at a pace that meets the demands within the DoD. Temporary waivers or work-arounds can prove counterproductive to the process.
2e. Establish a Red Team for independent assessments.	Some Red Team capabilities exist within the Services, NSA, and DIA.	Due to lack of clear policy and resources, aggressive, comprehensive, effective operational Red Team activities are lacking across DoD.
2e(1). Establish a Red Team which is accountable to SECDEF/DEPSECDEF and independent of design, acquisition, and operations activities.	No Red Team has been established to be directly accountable to the SECDEF/DEPSECDEF, independent of design, acquisition, and operations activities.	Without such an independent Red Team capability, current Red Team results may be questionable because of organizational affiliation/loyalties.
2e(2). Develop procedures for employment of the Red Team.	Thus far, the DoD has developed the Defensive Information Assurance Red Team (DIART) Manual.	Due to the lack of clear Red Team policy, there is no formal requirement for DIART to be implemented DoD-wide, and it is often ignored. This Red Team Manual provides the standardized procedures for any DoD Red Team, but absent a DoD Directive, there is no way to mandate their use. Additional, guidance needs to be provided on how results of the Red Teams (and any other assessment) are collected and analyzed to determine trends and lessons learned.

1996 Recommendation	Current Status	Current Shortfalls
3. Increase awareness. The SECDEF should:		
3a. Establish an internal and external IW-D awareness campaign for the public, industry, CINCs, Services, and Agencies	In June 1998 the ASD(C3I) and the USD(P&R) jointly issued a memorandum that required IW-D user awareness and training. There are currently numerous IW-D training activities throughout the DoD.	Conflicting definitions and usage related to IO, IA and CIP within the DoD and Intelligence Community causes resource and equity fights within the federal National Security Community and inhibits progress in resource management, training, and other important areas.
3b. Expand the IW Net Assessment recommended by the 1994 Summer Study to include assessing the vulnerabilities of the DII and NII.	Over the past five years, OSD - Net Assessment made several attempts to assess various aspects of IO. In each case, the assessment's value was limited by a lack of meaningful metrics. While the assessment could catalog and relate interesting anecdotal information, it would not provide the Secretary with the factual information necessary to make programmatic decisions. Accordingly, Net Assessment shifted its focus toward developing metrics by which the value of information under differing circumstances could be measured.	The IW Net Assessment has not yet been accomplished.
3c. Review joint doctrine for needed IW-D emphasis.	Joint Pub 3-13 (Defensive IO) was issued on October 9, 1998. CJCSI 6510.01B (Defensive IO Implementation), issued 26 August 1998, is currently under revision, with the new version expected to be issued in January 2001.	Doctrine and implementation instructions need to be adequately tested in exercises and integrated into mission planning and execution.
3d. Explore possibility of large-scale IW-D demonstrations for the purpose of understanding cascading effects and collecting data for simulations.	The Joint Staff and CINCs have sponsored exercises in which IW-D was a component.	It is unknown as to whether there have been large scale IW-D demonstrations conducted solely for the purpose of understanding the cascading effects and for collecting data for simulations. The modeling and simulation community lacks maturity in tools to assess these effects.
3e. Develop and implement simulations to demonstrate and play IW-D effects (USD(A&T) lead)	Current status is unknown.	Current status is unknown.

1996 Recommendation	Current Status	Current Shortfalls
3f. Implement policy to include IW-D realism in exercises.	The Joint Staff and CINCs have sponsored numerous exercises in which IW-D is a component. Exercise plans are increasing in sophistication to address these issues.	IW-D demonstrations do not effectively reflect cascading effects for collecting data for simulations.
3g. Conduct IW-D experiments.	DARPA and the C4I Joint Battle Center have conducted IW-D experiments.	It is unknown as to whether there have been large scale IW-D experiments conducted for the purpose of understanding cascading effects and collecting data.
4. Assess infrastructure dependencies and vulnerabilities. The SECDEF should:		There appears to be no overall DoD orchestrated approach to providing a strategic capability for DIO.
4a. Develop a process and metrics for assessing infrastructure dependency.	CIP (physical & cyber) analytical methodology has been identified and prototyped to link OPLANS / TPFDDs / Defense sector assets to analyze interdependencies	Prototype methodologies require thorough testing.
4b. Assess/document operations plans infrastructure dependencies.	CIP (physical & cyber) analytical methodology has been identified and prototyped to link OPLANS / TPFDDs / Defense sector assets to analyze interdependencies	Prototype methodologies require thorough testing.
4c. Assess/document functional infrastructure dependencies.	Defense infrastructure sectors are in the initial stages of performing sector characterization which will include intradependencies and interdependencies with other sectors	
4d. Assess infrastructure vulnerabilities.	DoD and JPO are beginning to develop protocol to include/integrate CIP (physical & cyber) assessments of defense infrastructures into existing assessment processes/procedures.	
4e. Develop a list of essential infrastructure protection needs.	Work in this area is currently ongoing.	No anticipated delivery date has been set for a final product/report.
4f. Develop and report to the SECDEF the resource estimates for essential infrastructure protection.	Estimates have been generated for initial CIP (physical & cyber) requirements to perform limited analysis and assessment.	Estimates must be refined, documented, and formally reported in order to promote appropriate action.

1996 Recommendation	Current Status	Current Shortfalls
4g. Review vulnerabilities of hardware and software embedded in weapons systems.	Not yet addressed. Recent changes in the DoD 5000 series and a Memo from USD(AT&L) adding security as an equal element to cost, schedule and performance for acquisition programs will assist in accomplishing this task. Reviews of some weapons systems were performed as a part of the Y2K effort and lessons learned should be incorporated.	<ul style="list-style-type: none"> • Lack of a formal requirement inhibits incentive to integrate these assessments into system development plans. • This area remains significantly vulnerable.
5. Define threat conditions and responses. The SECDEF should:		
5a. Define and promulgate a useful set of IW-D threat conditions which is coordinated with current intelligence community threat condition definitions.	INFOCONS have been established. CJCSI Memorandum of March 1999 served as vehicle for dissemination throughout the DoD. USSPACECOM is in the process of reviewing and revising the INFOCON process to make it more usable and ensure appropriate establishment and promulgation throughout DoD.	Interpretation of the INFOCONS varies within organizations, which can adversely impact their collective implementation.
5b. Define and implement responses to IW-D threat conditions.	Rules of engagement are currently undergoing legal review at Secret level.	DoD implementation of responses is hampered by existing and conflicting governing authorities and related rules of engagement.
5c. Explore legislative and regulatory implications.	Legislative and regulatory implications are currently being addressed through various activities within the federal government, as well as the DoD.	Current legislation and conflicting roles/responsibilities/authorities with the Department of Justice are impediments to the process.
6. Assess IW-D readiness. The SECDEF should:		
6a. Establish a standardized IW-D assessment system for use by CINCs, MilDeps, Services, and Combat Support Agencies.	CJCSI 6510.04 (Information Assurance Readiness Metrics), 15 May 2000, provides a standardized information assurance list of items to consider when preparing the information assurance portion within the JMRR C4 functional area.	There is no adequate system for assessing DIO readiness across DoD. CJCSI 6510.04 is relatively unknown within the Military Departments and, buried within the C4 functional area, has relatively little impact on assessing readiness. Although it establishes a baseline, it is neither mandatory, nor does it apply to all DoD activities.

1996 Recommendation	Current Status	Current Shortfalls
6b. Incorporate IW preparedness assessments in Joint Reporting System and Joint Doctrine, for example.	CJCSI 6510.04 (Information Assurance Readiness Metrics), 15 May 2000, provides a standardized information assurance list of items to consider when preparing the information assurance portion within the JMRR C4 functional area.	DIO is not adequately integrated into mission planning and execution. CJCSI 6510.04 is relatively unknown within the Military Departments and, buried within the C4 functional area, has relatively little impact on assessing readiness.
7. "Raise the bar" with high-payoff, low-cost items. The SECDEF should:		
7a. Direct the immediate use of approved products for access control as an interim until a MISSI solution is implemented and for those users not programmed to receive MISSI products.	NSTISSP No. 11, January 2000, requires that by 1 January 2002, acquisition of all COTS IA and IA-enabled IT products must be evaluated through the NIAP process. The NIAP provides a mechanism for certification of security products. NIST Special Publication 800-23 provides additional guidance in this area. In addition, the Defense in Depth strategy requires several levels of protection of networks and systems. Related security products include access control mechanisms (password control, PKI, biometrics), firewalls, intrusion detection devices, secure routers, etc.	
7b. Examine the feasibility of using approved products for identification and authentication.	The DoD PKI policy memorandum of May 1999 (replaced by the August 2000 Memo), establishes the DoD Public Key Infrastructure policy and Program Management Office (PMO). It establishes the desire to seek maximum use of COTS technology.	
7c. Require use of escrowed encryption for critical assets such as databases, program libraries, applications, and transaction logs to preclude rogue employees from locking up systems and networks.	Current DoD PKI policy addresses the use of escrowed encryption. The "insider threat" issue is being addressed by various efforts, one of which is through the Insider Threat IPT, which is looking at a spectrum of technical, policy, training, and other options to address this issue.	Systems Administrators have the "keys to the kingdom," yet often require no special "reliability" investigations, such as those in the Personnel Reliability Program.

1996 Recommendation	Current Status	Current Shortfalls
8. Establish and maintain a minimum essential information infrastructure. The SECDEF should:	Through the Y2K efforts, the DoD identified its minimum essential information systems ("thin-line"). This effort serves as a starting point for the CIP (physical & cyber) activities.	The critical infrastructures that are essential to the minimum operations of the economy and government are predominantly owned by the private sector. The DoD is extremely dependent upon these private sector systems, networks and infrastructures, but industry is not motivated to share information on their vulnerabilities with the government.
8a. Define options with associated costs and schedules.	Processes for defining and resolving associated funding requirements are under development.	
8b. Identify minimum essential conventional force structure and supporting information infrastructure needs.	Addressed, in part, in JV2010 and JV2020.	Significant personnel resource shortfalls impact execution of the DIO mission at all levels in DoD.
8c. Prioritize critical functions and infrastructure dependencies.	Under development.	No final product/report or due date has been defined or funding applied.
8d. Design a <u>Defense</u> MEII and a failsafe restoration capability.	The CIO organization is applying lessons learned from the Y2K experience in registering applications, determining mission critical/mission support and policies concerning NIPRNET access.	
8e. Issue direction to the Defense Components to fence funds for a Defense MEII and failsafe restoration capability.	No guidance issued to date.	The DoD continues to remain vulnerable.
9. Focus the R&D. The SECDEF should focus the DoD R&D program on the following areas:	The DIAP Research & Technology (R&T) functional area was established to provide focus in the DoD IA R&D areas. This functional area works primarily with the InfoSec Research Council (IRC), a voluntary member organization of a number of activities (DoD and non-DoD), doing IA research.	

1996 Recommendation	Current Status	Current Shortfalls
9a. Develop robust survivable system architectures.	DARPA sponsored major program in this area.	<ul style="list-style-type: none"> • The DoD is managing its current information assurance R&D in a fragmented way that is not sufficiently focused on the information assurance requirements of the GIG. • The current DoD network architecture calls for a secure network with authorized access via tokens (i.e., PKI). The scope of this security apparatus is enormous, and PKI has not been modeled and tested under extreme requirements.
9b. Develop techniques and tools for modeling, monitoring, and management of large-scale distributed/networked systems.	Previous and ongoing IA R&D efforts are addressing this area.	Development and deployment of new network technology has greatly outpaced information assurance technology, thereby increasing the vulnerability of DoD systems.
9c. Develop tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks.	Previous and ongoing IA R&D efforts are addressing this area.	<ul style="list-style-type: none"> • One of the weakest aspects of U.S. DIO is our extremely limited ability to detect, assess, and understand both hostile IO capabilities and precursor indications and warning of attack. • No methods exist for automated or assisted discovery of existing or novel attack patterns or signatures, particularly for those attacks which are distributed across many computers or networks. • Intrusion detection technologies currently produce only moderately reliable results in simple environments, and even less reliable results in complex environments.
9d. Develop tools for synthesizing and projecting the anticipated performance of survivable distributed systems.	Previous and ongoing IA R&D efforts are address this area.	DoD does not have a methodology for restoring integrity in its systems.
9e. Develop tools and environments for IW-D oriented operational training.	The Joint Battle Center is chartered to perform this work and has a number of on-going activities to address issues in this area.	The DoD is not aggressively or innovatively addressing its IA R&D personnel requirements, which will likely lead to more serious problems in the next few years as more personnel leave the department and fewer high caliber R&D managers remain.

1996 Recommendation	Current Status	Current Shortfalls
9f. Develop testbeds and simulation-based mechanisms for evaluating emerging IW-D technology and tactics.	Previous and ongoing IA R&D efforts are address this area.	Progress in defending and protecting the GIG will require a far greater ability to model and simulate the performance of information infrastructures than we have today.
9g. The SECDEF should work with the NSF to develop research in U.S. computer science and computer engineering programs.	NSA's Information System Security Engineering program is working with 7 universities in this area.	This NSA program is independent and not implemented with NSF.
9h. The SECDEF should work with the NSF to develop educational programs for curriculum development at the undergraduate and graduate levels in resilient system design practices.	NSA's Information System Security Engineering program is working with 7 universities in this area.	The degree to which the NSA program, which is implemented independent of NSF, is addressing curriculum development is unknown.
10. Staff for success. The SECDEF should:		
10a. Establish a career path and mandate training and certification of systems and network administrators.	An IT/IA Human Resources IPT was established to examine issues associated with the establishment of an IA/IO career path. An OSD memorandum in June 1998 addressed mandatory training.	The shortage of DoD IT professionals is serious and growing.
10b. Establish a military skill specialty for IW-D.	Skill specialties have yet to be established. The Joint Staff has a tasking to develop common skill sets for specific functions in this area. The military Services have all undergone major restructuring of their military skill sets to identify, recruit and retain professionals in this area.	The appropriate staffing of DIO positions continues to be severely hampered.
10c. Develop specific IW awareness courses with strong focus on operational preparedness in DoD's professional schools.	There are numerous activities in this area. IA awareness products and activities, and IA/IO courses, are provided at all professional military education facilities.	The DoD workforce at all levels is ill prepared to execute the DIO mission because current training efforts are fragmented, inadequately scoped, and poorly documented.

1996 Recommendation	Current Status	Current Shortfalls
<p>11. Resolve the legal issues. The SECDEF should:</p> <p>11a. Promulgate for Department of Defense systems:</p> <ul style="list-style-type: none"> Guidance and unequivocal authority for Department users to monitor, record data, and repel intruders in computer systems for self protection. Direction to use banners that make it clear the Department's presumption that intruders have hostile intent and warn that the Department will take the appropriate response. IW-D rules of engagement for self-protection (including active response) and civil infrastructure support. 	<ul style="list-style-type: none"> Legal guidance has been promulgated and policies are under review regarding the monitoring and auditing of network activities. Intrusion Detection Systems perform a portion of this function. Guidance on configuration of the various devices is provided as technology changes. Additional mechanisms to identify and warn intruders are being investigated, as well as a general announcement of DoD policy and intent through the normal media channels. Rules of engagement issues, including active defense are being investigated to determine possible actions. 	<p>The use of banners can only address the "insider issue." Intruders into systems generally bypass standard entry routes and it is virtually impossible to set up mechanisms for banners to be present on all entry points.</p>

1996 Recommendation	Current Status	Current Shortfalls
<p>11b. Provide to the Presidential Commission on Critical Infrastructure Protection proposed legislation, regulation, or executive orders for defending other systems.</p>	<p>OBE, since PDD 63 was signed. However, there are a number of ongoing legislative activities being addressed among the NIPC, Federal CIO Council, and the CIAO.</p>	<ul style="list-style-type: none"> • The DoD is suffering under existing legislation. Although it has the responsibility for national defense, it has been forced to rely on law enforcement agencies such as the FBI and the Justice Department to gather information about attacks. • Under existing law, network service providers may give away information about hacking attacks to the public, but they are legally prohibited from giving the information to a government agency unless the agency begins a criminal investigation. • There is no clear guidance as to which takes precedence: the confidentiality of criminal investigations or the national security interests of the United States. • Criminal wiretap authorities are inadequate for the government to maintain wiretap coverage of persons engaged in long-term hacking campaigns against government networks. • Current law concerning "trap and trace" orders often requires that law enforcement agencies seek multiple, sequential orders as they trace a single hacker from system to system.
<p>12. Participate fully in critical infrastructure protection. Regarding the activities of the President's Commission on Critical Infrastructure Protection, the SECDEF should:</p> <p>12a. Offer specific Department capabilities to the President's Commission.</p>	<p>OBE, since PDD 63 was signed. However, there are a number of activities in the CIP area that are working with the CIAO to address the spirit of this recommendation.</p>	

1996 Recommendation	Current Status	Current Shortfalls
12b. Advocate the Department's interests to the President's Commission.	OBE, since PDD 63 was signed. However, there are a number of activities in the CIP area that are working with the CIAO to address the spirit of this recommendation.	<ul style="list-style-type: none"> • No one has the responsibility or authority to make response and recovery decisions and take actions across stovepipes. Coordination depends upon personalities. • The State Department is potentially very important to DIO, but is not sufficiently engaged. • A great portion of government doesn't understand DIO issues or appreciate the potential impact of information technology vulnerabilities on their operations.
12c. Request the Commission provide certain national-level capabilities for the Department.	OBE, since PDD 63 was signed. However, the NIPC, for which the DoD provides personnel resources, provides the law enforcement capabilities.	<ul style="list-style-type: none"> • There is no clear responsibility for rationalizing law enforcement and national defense equities when certain types of cyber attack are detected. • There is currently a bias toward using law enforcement authorities and procedures when a cyber incident is detected. Although this will be satisfactory in the vast majority of cases, no formal means exists to review cases to determine if national security procedures might be more appropriate.
12d. Suggest IW-D roles for government and the private sector.	OBE, since PDD 63 was signed. PDD 63 established roles and responsibilities.	
13. Provide the resources. Develop a plan and associated budget beginning in FY97 to obtain needed IW-D capability (ASD(C3I) lead)	The DIAP is currently attempting to obtain IW-D funding requirements from DoD organizations. With the improved visibility into DoD component budgets, areas requiring additional funding are being identified. The DIAP has established appropriate mechanisms through the PPBS process to identify and justify shortfalls – the issue is how to prioritize and obtain additional funding in a tight budget environment.	The Department has not sufficiently funded protection of its networks and DIO programs. Of particular concern in the Sensitive, But Unclassified (SBU) information, which is critical to JV2020.

ANNEX G

Defense Science Board Task Force on Defensive Information Operations

Thought Pieces

- | | |
|----------------|--|
| TAB G-1 | Oversight and Management of the
GIG Executive Director |
| TAB G-2 | The Problem Continuum from Data to Understanding |
| TAB G-3 | The Insider Threat & The Low and Slow Attack |
| TAB G-4 | Red Teaming and the Cyber Operations Readiness
Triad (CORT) |

ISSUE PAPER

OVERSIGHT AND MANAGEMENT OF THE GIG EXECUTIVE DIRECTOR

Issue: Why the CIO Executive Board and the MCEB are not the right management vehicles to provide oversight and governance for the GIG Executive Director as recommended by the DIO DSB.

Background: The DIO DSB has recommended that at DoD "Information Superiority" Board of Directors (BoD) be established to provide oversight and governance for the GIG Executive Director, an office which would provide systems engineering resources for the Global Information Grid. The membership of this BoD would consist of: Chair, DEPSECDEF, USD(AT&L), Vice Chairman of the Joint Chiefs of Staff, ASD(C3I), and the DDCI.

Discussion:

- **DoD CIO Executive Board:** The current charter of the DoD CIO Executive Board is contained in the DEPSECDEF Memo Subj: DoD Chief Information Officer Executive Board, 31 March 2000. This charter states that the Council is the principal forum to advise the DoD CIO on the full range of matters pertaining to the Clinger-Cohen Act (CCA) of 1996 and the Global Information Grid. Additionally, the Board also coordinates implementation of activities under the CCA, and exchanges pertinent information and discusses issues regarding the GIG, including DoD information management (IM) and information technology (IT). The primary mission of the Board is to "advance the DoD's goals in the areas of IM, information interoperability and information security between and among Defense Components." The Board also coordinates with the IC CIO Executive Council on matters of mutual interest pertaining to the GIG. Its management oversight includes recommending, reviewing and advising the DoD CIO on overall DoD IM policy, processes, procedures and standards, as well as to oversee all aspects of the GIG to support the DoD's and IC's mission and business applications. This includes the collaborative development of IT architectures and related compliance reviews; management of the information infrastructure resources as a portfolio of investments; collaborative development of planning guidance for the operation and use of the GIG; and identification of opportunities for cross-functional and/or cross-Component cooperation in IM and in using IT. The Board's Architecture Management responsibilities include ensuring the collaborative development of architectures as specified in the CCA, and ensuring that processes are in place to enforce their standardized use, management and control, as well as aligning IT portfolios with the GIG. Although the Board has budgetary review authority for IT investments, and can make recommendations, it has no direct budgetary authority. It also has no authority, either review or management oversight into the warrior components of the GIG. The membership of the DoD CIO Executive Board includes:

- Chair: DoD CIO (ASD(C3I))
 - Members: CIOs of the Military Departments
 - CIO, Joint Staff
 - USD(AT&L)
 - USD (P) (Policy)
 - USD (C) (Comptroller)
 - USD(P&R) (Personnel and Readiness)
 - ASD (C3I) (usually the Deputy CIO)
 - Director PA&E (Program Analysis and Evaluation)
 - J6, Joint Staff
 - OPNAV N6
 - Director, Communications and Information, USAF, AF/SC
 - IC CIO
 - CIO, JFCOM (Joint Forces Command)
 - Security Advisor: DIRNSA
 - Technical Advisor: Director, DISA
 - Legal Advisor: DoD General Counsel
- **MCEB:** The charter of the MCEB is contained within DODDIR 5100.35 dtd 10 Mar 1998. The MCEB is supposed to consider those military communications-electronic matters, including those associated with National Security Systems(NSS) referred to it by the SECDEF, CJCS, the DoD CIO, Secretaries of the Military Departments, and Heads of DoD Components. The mission of the MCEB is to obtain coordination among the DoD components, between the Department of Defense and other Governmental Departments and Agencies and between the DoD and representatives of foreign nations on matters under the MCEB jurisdiction. The MCEB provides guidance and direction to the DoD components and advice and assistance as requested. The membership, as listed below, is primarily the communications activities in the listed components, who have little, if any, authority over IT issues in other portions of their component. The MCEB has no budgetary review or execution authority over any component, nor is there any mechanism within the MCEB structure for enforcement of non-compliance with decisions. The relationship between the MCEB and CIO Executive Board is still being discussed, but in effect, the MCEB is a subordinate activity under the direction of the CIO Executive Board and recommendations referred to that Board for final decision. Membership of the MCEB includes:
- Chair: Joint Staff, J6
 - Members: Vice, J6
 - DISC4, U.S. Army
 - OPNAV, N6
 - HQ USAF, SC
 - HQMC, C4
 - USCG, Assistant Commandant for Systems

Director, DISA
Director, NSA
Director, DIA

- **General:** Neither the DOD CIO Executive Board nor the MCEB have the membership or authority over budgets and execution activities envisioned as necessary to ensure the GIG is built and managed as intended. Without that level of authority over all elements of the GIG, the architecture is subject to interpretation by each component based on their needs, rather than the needs of the entire organization. There is also little incentive to address cross-cutting issues in a coherent fashion when the funding for these programs is provided via Title 10 channels without some mechanism to force cooperation. Because of the Title 10 and DoD versus Intelligence Community issues, the only level of management senior enough to cross this bridge is at the DEPSECDEF level. Additionally, neither of these two boards has a direct oversight responsibility over any specific office or function which carries out its direction such as the relationship described between the GIG Executive Director's office (a function which does not currently exist) and the DoD "Information Superiority" Board of Directors.

Recommendation: That a body as described for the DoD "Information Superiority" Board of Directors be established to provide oversight for the implementation of the GIG. With the establishment of such a body, the relationship with existing organizations (i.e. CIO Executive Board and MCEB) must be defined and roles, missions and responsibilities clarified.

THE PROBLEM CONTINUUM – FROM DATA TO UNDERSTANDING

One problem of great concern in today's information age, is the overwhelming volume of data and information readily available over the Internet and through the wide range of sensors that support DoD activities. The push to provide more information to the commander in the field has many commanders concerned that they will be so overwhelmed with data and information that it may actually impede the decision making process.

The key to remedying this problem is recognizing and enabling the transition from data, to information, to knowledge, and ultimately to understanding. The concept of "Decision Superiority" put forth in Joint Vision 2020 requires a greater level of understanding in order to make timely and accurate decisions. DoD must identify those technologies and tools that will ensure the rapid transition from data to understanding, investing today, to build a capability that will enable Joint Vision 2020. Simply pumping more data to the front lines is not the answer. Joint Vision 2020 necessitates a more balanced approach including:

- Decreased dependence on data.
- Increased ability to identify key information.
- Larger degree of knowledge based on key information.
- Clear understanding of the information picture in order to gain and maintain Decision Superiority.

The variety of available and soon-to-be available tools and technologies that support this effort is staggering. Visualization, analysis, and security tools are the centerpiece of the technologies that will enable this transition from data to understanding. Specific categories worthy of investigation include:

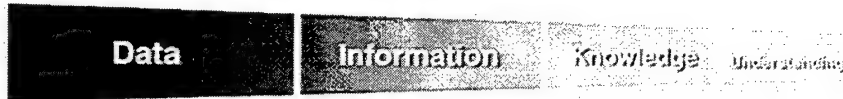
- Visualization Tools:
 - Data mining
 - Data warehousing
 - Pattern recognition
 - Profile search agents
- Analysis Tools:
 - Modeling & Simulation
 - Automated data analysis

- Security Tools:
 - Intrusion detection
 - Key control
 - Data filtering

The enclosed slides, developed in support of the 1999 Defense Science Board Summer Study, provide further clarification of these critical areas, and the critical transition from data to understanding.

What We Have vs. What We Need

- Information Superiority, like information assurance, is dependent on taking a large volume of data, sifting through it to gain key information, leading to knowledge that can be applied as understanding.
- What We Have:



- Today, the US can gather a vast amount of data through a variety of sources and sensors.
- Some of that data can be sifted to find the nuggets of key information.
- A lesser amount is converted to knowledge, and even less is really understood.

What We Have vs. What We Need

What We Need: A More Balanced Approach...

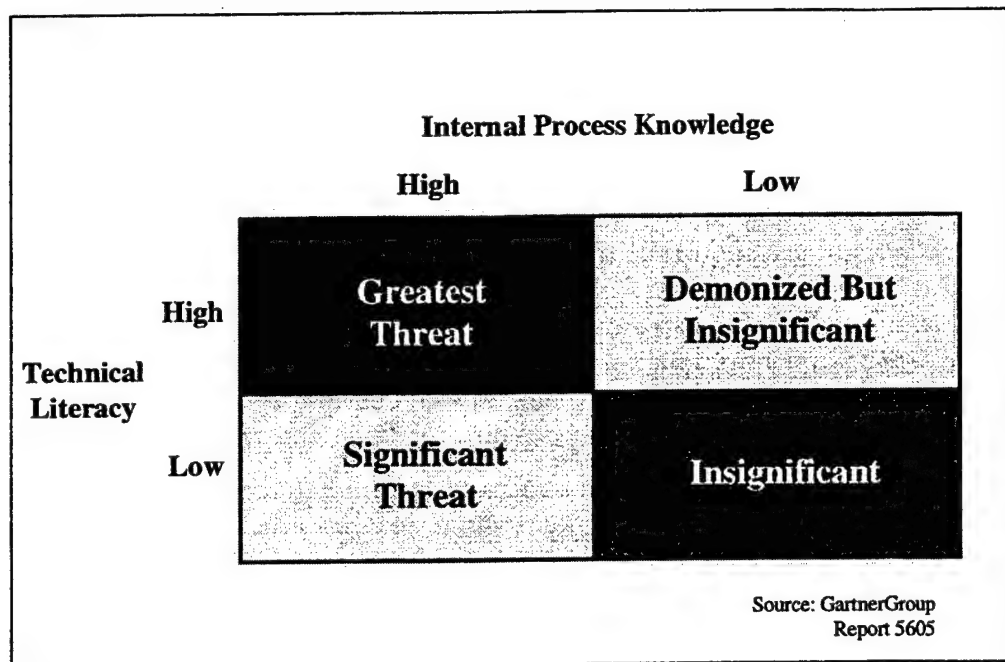
Data	Information	Knowledge	Understanding
-------------	--------------------	------------------	----------------------

- **Decreased dependence on data.**
- **Increased ability to identify key information.**
- **Larger degree of knowledge based on key information**
- **Clear understanding of the information picture in order to gain and maintain Information Superiority.**

THE INSIDER THREAT & THE LOW AND SLOW ATTACK

The threat to U.S. information systems is becoming more and more prevalent as state sponsored terrorists, nation states, and organized crime groups enter the world of cyber warfare. Perhaps the most dangerous threat, however, is the insider and the low and slow attack.

The GartnerGroup published a report in October, 1999, entitled "Information Security Hits the Front Page: How Safe is Safe Enough?" One of the central themes of that report was the danger and likelihood of the insider threat. The following graphic, extracted from the report, demonstrates their conclusions:



The key is as follows:

- 1) A person with low technical literacy and low internal knowledge is an insignificant threat (bottom right box).
- 2) A person with high technical literacy and low internal knowledge can be a bother (demonized) but is insignificant (top right box).
- 3) However, a person with low technical literacy and high internal knowledge (the "dumb" insider) is a significant threat (bottom left box).

- 4) Finally, a person with high technical literacy and high internal knowledge (the "smart" insider) is the greatest threat (top left box).

DoD released the "Insider Threat Mitigation Report" in April, 2000, citing this threat as "real, and very significant." The report cites four basic sources of insider security problems:

- Maliciousness
- Disdain of security practices
- Carelessness
- Ignorance

The report further states that the majority of insiders "are hardworking and dedicated to their professions" and "understand the importance of their work to the nation." The greatest concern, however, is the significant damage a single "malicious" insider could cause. The report continues by stating, "The insider has the capability to disrupt interconnected DOD information systems, to deny the use of information systems and data to other insiders, and to remove, alter or destroy information. Consequently, the insider who betrays the authorities, trust and privileges granted to them may be aided in their malicious activity by the very information systems upon which the department depends."

The report also addresses the Defense Department's heavy reliance on commercial off-the-shelf information systems, adding to the complexities in detecting and dealing with insider threats. The report contends that DoD "has little or no knowledge of who developed the systems and, therefore, no measure of the trustworthiness, reliabilities or loyalties of those individuals". The report acknowledges that individual developers of COTS products "would have an extraordinarily difficult task to target a particular customer because COTS products tend to be produced in large quantities and shipped to customers as an activity that is independent of the individual developer. However, the potential for accepting an error-filled COTS system is real, and demonstrates that "cyber-outsiders can quickly attain many characteristics of an insider".

When this type of infrastructure is attacked from the inside, the results can be catastrophic. The knowledgeable insider has the know-how and the access to delete, modify, or transfer critical data, and may be capable of affecting hardware capabilities through inside attack as well. Add the potential for the low and slow attack, and most network security systems are not capable of detecting unauthorized activity. The low and slow attack is an instance where the attacker uses low visibility access and may not expect or require results for an extended period of time. Data transfers or modifications may be time delayed until the time of the attacker's choosing, or trap doors and trojan horses may be installed for subsequent execution.

The problem is further complicated by the frequent focus toward a perimeter defense mentality to keep out unwanted outsiders, based on the well-published concerns about outside hacker attacks and cyber-terrorism. The real issue is the fact that all of those technological safeguards designed to keep hostile computer attacks out won't help with the disgruntled insider.

Government (GAO) statistics indicate that the average cost of an outside hacking incident was \$57,000, while the average cost for a serious insider hacking incident was \$2.7 million. This discrepancy merits serious attention if DoD is to have any hope of securing its networks.

**“THE CYBER OPERATIONS READINESS TRIAD (CORT)”
VULNERABILITY ASSESSMENTS (VA)
VULNERABILITY EVALUATIONS (VE)
RED TEAMING (RT)**

BACKGROUND:

Recently, ASD(C3I) has asked where the Discover Vulnerabilities (DV) process and IO Red Teaming fits into the larger picture of DoD “force readiness protection” and Defensive Information Operations (DIO). ASD(C3I) has also asked the question; “Does DoD actually have a standing DIO Red Team? The answer to that question is yes. NSA is DoD’s Red Team, and is the team of choice to do adversarial Red Teaming within DoD. The larger issue of a total look at cyber force readiness as well as Red Teaming is a timely one as the DV process begins to take shape in DoD. Questions like, where does DV belongs in DoD; who is the lead organization; who leads overall technical training of the force; how do we measure readiness; what are the standards/metrics for Readiness; and the question of Defense contractors assisting in meeting the extensive tasking are of importance.

PURPOSE:

This white paper will describe:

- The existing discover vulnerability (DV) process within NSA, recommendations for potential modification to the process, and a possible win-win solution to current operations with regard to the use of the civilian contracting community.
- The IO Red Team process, it’s role in force readiness protection and Defensive Information Operations (DIO) and what Red Teaming could evolve to based on NSA’s experiences from Eligible Receiver (ER) and the 40+ exercises conducted since then.

DISCUSSION:

NSA and the Services.

The NSA Red Team, as part of NSA’s Information Systems Security Organization’s (ISSO) mission, is to improve the Operational Readiness (OR) & Defensive Information Operations (DIO) posture of DoD and it’s components. The NSA Red Team is an interdisciplinary and sophisticated “opposing force” (OPFOR) that utilizes active and passive, as well as technical and non-technical capabilities to expose and exploit customer IO vulnerabilities in order to improve

operational readiness. Based on Red Team findings, timely feedback is provided directly to the customer consisting of their vulnerabilities as well as specific recommendations and countermeasures to thwart potential real-world exploitation of their computer and network systems.

Organizations "stressed" by NSA's Red Team operations gain a sense of their general cyber readiness by measuring effectiveness in protection, detection, response, and reconstitution during Red Team exercises. Upon customer request and negotiated between the customer and the NSA Red Team (also incorporated into the "Rules of Engagement" (ROE)), the NSA Red Team may use cooperative partners & alliances to work as a true OPFOR covering more than one pillar of IO. In the past, the NSA Red Team has partnered with other internal NSA organizations, as well as CIA, DIA, JTF/CND, NIPC, DHS, AFTWC, LIWA, FIWC, SOCOM, and the Military Services.

It is an over statement to say that the readiness posture of individual DoD organizations varies widely across the Department. Some of the component organizations within the CINCs, Services, or Agencies maintain highly effective DIO programs, while others place less emphasis on securing of their networks. Reasons vary for this dilemma, but are telling. For the Services, the total number of people who are highly skilled at discovering and exploiting vulnerabilities remains small, and their time and efforts must be managed wisely. Further, the quantities of such persons are uneven across the Services. For this reason, the Services play up to their strengths, offering a range of assessment services that maximizes their skill usage. The bottom line for the Services is that they cannot yet muster the critical mass of personnel skilled in the area of DV. The CINC's are not in much better shape, as they draw on the Military Services for their technical manpower. Currently, NSA is the only DoD entity that has the ability to focus full-time on computer **and** network vulnerability discovery at all levels of the process. It is NSA's view that it should be designated as DoD's EA for Discovering Vulnerabilities (DV). We have the talent and know-how to organize DoD in the DV process. However, it is also our view that the DV process requires refocus and a relook on where DoD needs to concentrate limited.

THE PROCESS:

We see the DV methodology as a cyclic process composed of 3-levels of service surrounded by OPSEC. The process is called "THE CYBER OPERATIONS READINESS TRIAD (CORT), and it's main goal is to improve the cyber security of DoD. The initial level, called a Vulnerability Assessment or Infosec Assessment, provides a high-level review of a customer's automated information system (AIS) security policies, plans, and procedures to determine if a minimal level of protection is in place. This is what is known as a Level 1 assessment. No legal authority is required to conduct this assessment. These people are responsible to support DoD and DoD/NII-associated partners. Due to increased customer request for this service, and working with the National Institute of Standards (NIST) and the DIAP, we have initiated the Information Security System Capabilities Maturity Model (ISS-CMM) process. This process invites the Defense contracting community to become "authorized", via a validated training program, to conduct Level 1 assessments to the same level as NSA. The only difference in the end result is the customer and Contractor negotiate a price for the assessment conducted. For this level of assessment, the contracting community is technically suited to conduct level 1 assessments and is a workable solution to PDD-63 customer concern over DoD evaluators in

their systems. The second level of assessment (Level II) is called a Security or Vulnerability Evaluation. This process looks past the basics and provides an in-depth technical analysis of a customer's information system(s). The objective is to identify *any and all* vulnerabilities (not just those associated with a specific threat agent) and assist the customer organization in addressing them. This type of DV evaluation requires NSA general counsel (AGC(I)) and DDI approval to touch a DoD customers networks or computer systems. In order for final approval, the customer must meet certain criteria and standards when requesting NSA to actually "touch" the network. This is an extremely technical operation and requires a certain skill-set to complete the task. Heretofore, NSA has been the only DoD element to conduct this in depth testing on a system or network. It is our experience that the Military Service elements conduct varying degrees of Level 1 and Vulnerability Evaluations and each conducts these services to a component with their own set of standards. IO Red Teaming is the third (Level III) and final level of service. It is *normally* reserved for larger DoD elements and other customers who are looking to test their networks and cyber security in an exercise environment, either as a no-notice Red Team-only evolution or as part of a larger exercise; e.g., the Marine exercise URBAN WARRIOR. SECDEF approval is required to conduct these operations and due to the complexity and technical nature of Red Teaming operations, NSA remain the only operative element to conduct this type of Red Teaming. Further dialogue is required to come to closure on where the Military Services and the Defense Contracting community play in the Vulnerability Evaluation (Level II) process and Red Teaming and what standards/metrics are required.

Once Red Teaming is performed on a system and/or network(s), the customer would optimally reevaluate where they are in their respective security environment and then via the Vulnerability Assessment Vulnerability Evaluation, or Red Teaming process, relook at what is required to secure their networks. This continuous process is a strong and proven force in "raising the bar for readiness" on computer and network security. It is this paradigm under which the NSA DV process operates, and that we believe should be required within all DoD Components.

DEFINITION:

A Red Team, as defined in the draft of DoD Directive 3600.3 "DoD Information Operations Red Teaming" is:

"An independent, threat-based, and simulated opposition force that uses passive, active, technical, and non-technical capabilities on a formal, time-bounded basis to expose and exploit information system vulnerabilities of friendly forces."

The directive further states that:

"The goal of Red Teaming is to improve the readiness and defensive IO posture of DoD Components."

In general, a large portion of the Defense community concurs with the DV process, however, there remains many entities throughout the Department, other government agencies, and the private sector who do not subscribe to, define as, or conform to conducting vulnerability discovery in this manner. It is our sense that the DV process be standardized across the board.

Should NSA be given the EA responsibility for DV in general, it is our view that we would further refine and adjust the process for use in DoD.

THE PRIVATE SECTOR:

The DV process covers three levels of service. We believe the private sector can play a pivotal role in filling the Departments needs in the DV process where we (NSA, DoD Services, Agencies, etc) are over tasked and lacking, in some areas, skilled personnel. It is our sense that the VA and VE process, where appropriate, can be assisted by the Defense contracting community if trained and certified appropriately. Although a relatively new endeavor, the ISS-CMM for the VA process is proving a workable alternative. Equally, we believe if structured properly, and a system set up to assure the results are equal to the existing VE process, that private sector could assist in that part of the DV process, as well. However, NSA has not yet initiated an effort to begin the training and certification process for vulnerability evaluation (level II) work. If tasked, the strategy is to slowly build-up competencies for Level I assessments within Industry, and then grow additional expertise from there. Our vision is to ultimately *share* with the private sector requirements for Level II evaluations. (I deleted the last sentence)

With regard to Red Teaming, we believe there should be measured involvement by the Defense Contracting community. Contractors are involved in Red Teaming now, however, only as working under NSA authorities. There may come a time, because of the growing concern over cyberattack that we reevaluate contractor play across the board as it applies to Red Teaming. The Red Team is an opposing force. We "attack" U.S. systems. We succeed at breaking into U.S. systems. We have a very elaborate structure in place to handle our mission and/or if our mission goes awry. We have a trusted agent network, deconfliction process, classified tools and techniques, access to real world threat and resource information, sophisticated laboratory testing procedures, cover program, legal authorities and most importantly, a dedicated cadre and critical mass of career personnel with TS/SCI clearances. It also should be stated that we are creating lasting relationships & liaisons with other military departments, Agencies, and others that would simply be extremely difficult for private industry to emulate. Lastly, the "trust and ethical" issues would be most acute. We do not believe that system owners of the most sensitive DoD networks (SIPRNET, JWICS, etc) would feel comfortable with private industry performing the DoD's most sensitive vulnerability evaluations without a DoD cover or operational authority. Since this service is performed at the local as well as the "remoted" level, we envision huge conflicts with private industry performing such services, since they do not have the legal authority to use "jump-points" throughout DoD networks and Agencies.

Exercise planning for Red teaming in the outyears:

Fiscal Year	FY-00	FY-01	FY-02	FY-03	FY-04	FY-05	FY-06	FY07
Major Exercises(CINC-level)	4	8	10	12	14	14	14	14
Minor Exercises	4	6	8	10	10	10	10	10

CONCLUSION:

IO capabilities of DoD's adversaries are growing and becoming more sophisticated. These adversaries include hackers and other unstructured groups intent on supporting political objectives, and structured groups such as terrorists, rogue nations, or nation states. In addition, the strategies of our adversaries are becoming increasingly clever, drawing from across the spectrum of IO techniques. With the growing number of hacking groups and the ease with which a terrorist group or nation state can obtain the tools necessary to conduct an IO campaign, the threat is harder to identify and stop without proper training and readiness. It is essential that the United States have the capability and experience necessary to counter such threats. Issues such as Solar Sunrise, which almost stopped a US troop deployment, the I Love You Virus, as well as the well publicized intrusion called Moonlight Maze, highlight just some of the growing threats. Red Teams and the DV process can "hone" the DoD's DIO capability and provide the experience required to enhance the security awareness and readiness posture; necessary elements to dominate in conflicts where IO represents a strategic advantage.

ANNEX H

Defense Science Board Task Force on Defensive Information Operations

Reference Data

TAB H-1	CERT and IO POC Listings
TAB H-2	Terms of Reference

CERT AND IO POC LISTINGS

Name	Function/Constituency	E-Mail/WWW URL
AFIWC - Air Force Information Warfare Center	USAF IW coordination and support to the Numbered Air Forces (in addition to the IO-Flights assigned directly)	http://www.afiwcc.aia.af.mil/ http://www.afcert.csap.af.mil/
ANSIR - Awareness of National Security Issues and Response (FBI)	Subset of NIPC providing advisories for corporate security professionals (subscribable messaging)	http://www.leo.gov/gharter@leo.gov http://www.fbi.gov/ansir.htm
ASD(C3I) - Assistant Secretary of Defense for Command, Control, Computers, and Intelligence	Principal advisor to the President for C3I	http://www.c3i.osd.mil/
CIA - Central Intelligence Agency	Office of Transnational Issues (OTI) Clandestine Information Technical Office (CITO)	http://www.odci.gov/cia/
CIAO -- Critical Infrastructure Assistance Office	Formed from President's Commission on Critical Infrastructure Protection. Site provides text and summary of PDD 62/63, and related policy papers	http://www.ciao.gov/
CND-JTF - Computer Network Defense Joint Task Force	Task force on DoD Computer Network Defense	jtfwo@assist.disa.smil.mil
DARPA - Defense Advanced Research Project Agency	DoD specialized advanced research projects	http://www.darpa.mil/

TAB H-1

DIA – Defense Intelligence Agency	IPB for IW / STO coordination & Defensive IO Transnational Warfare Issues (TW) Branch & Information Warfare Support Office (TWI)	http://www.odci.gov/ic/usic/dia.htm
DISA – Defense Information Systems Agency	DoD agency responsible for information technology; central manager for the DII; Answers to ASD(C3I) Center for Information Systems Security (CISS) Automated System Security Incident Support Team (ASSIST)	http://www.disa.mil/ http://www.disa.mil/ciss/index.html http://www.assist.mil/ http://www.fiwc.navy.mil/
FIWC – Fleet Information Warfare Center	Operational IW/C2W support to the fleet (Norfolk and San Diego)	
IOTC – Information Operations Technology Center	DoD/DCI center at Ft Meade focused on technology trends (not geographic) for IO Advanced Tech Group (ATG) Analysis & Assess Grp (AAG) Community Coordination Group (CCG)	
ITAC -- Infosec Technical Assistance Center	Navy Infosec assistance service	itac@infosec.navy.mil
JC2WC – Joint Command and Control Warfare Center	Joint support to IO/C2W Located at Kelly AFB, San Antonio	

JCS J2	Intelligence; Deputy Dir for Targets (J2T)	http://www.dtic.mil/jcs/
JCS J3	Operations; J39: Deputy Director for IO	http://www.dtic.mil/jcs/
JCS J6	C4; Information Assurance Div	http://www.dtic.mil/jcs/
JCS J8	Force Structure; Joint Warfighting Capabilities Assessment (JWCA)	http://www.dtic.mil/jcs/
JPO - Joint Program Office	Internal US vulnerability assessments	
JSC - Joint Spectrum Center	Management of the electromagnetic spectrum	http://www.jsc.mil/
JWAC - Joint Warfare Analysis Center	External vulnerability assessments; infrastructure & IO focus	http://www.jwac.ic.gov/
LIWA - Land Information Warfare Activity	Army IO coordination and field support	Site under revision
MITRE Corp	FFRDC providing IO-related analysis, and C2 systems analysis	http://www.mitre.org/ corpc@mitre.org
NGIC - National Ground Intelligence Center	Provides Army intelligence support to IO: Ground Crisis Action Team; IW Ground Control Team; Army CI Center	
NIPC - National Infrastructure Protection Center	Critical infrastructure protection (FBI&Other agencies)	nipc@fbi.gov http://www.nipc.gov/
NRO -- National Recon. Office	Space recon systems; Global information superiority	http://www.nro.odci.gov/

NIST -- National Institute of Standards & Technology	Technical measures and standards coordinated with industry	http://www.nist.gov/
NIWA -- Naval Information Warfare Activity	Naval lab support to IW; fielding IW systems; assessing vulnerabilities; IW mod/sim	
NSA -- National Security Agency	Infosec; Encryption; Information System Security Organization (ISSO)	http://www.nas.gov/ www.nsa.gov:8080 http://www.defenselink.mil/pubs/almanac/osd.html
OSD-NA -- Office of the Secretary of Defense for Net Assessment	Assessments on a variety of US vs Other capabilities, including IO/IW	
PM-IW -- Program Manager for Information Warfare (Army)	Army acquisition program manager for IW	No web site available
RAND Corp	FFRDC providing C2 systems analysis and integration; focusing on production, distribution, and safeguarding of intelligence information	http://www.rand.org/
USD(C) US Department of Commerce	Trade issues related to IO	http://www.doc.gov/
USD(J) -- US Department of Justice	Legal issues related to IO and FBI involvement	http://www.usdoj.gov/
USD-P -- Under Secretary of Defense for Policy	Policy advise for IO and ROE	http://www.defenselink.mil/pubs/almanac/osd.html
USD(S) -- US Department of State	Foreign policy including IO related issues	http://www.state.gov/

USCENTCOM US Central Command	J33 - IO Cell	http://www.centcom.mil/
USSOCOM - US Special Operations Command	Special Operations - Information Operations Office (SOIO)	http://www.socom.mil/
USSOUTHCOM - US Southern Command	J33 - IO Cell	http://www.ussouthcom.com/southcom

LABS

ARL - Army Research Lab	Electronic Warfare, Directed Energy, and Electronic Countermeasures research; Information Science and Technology Branch (IS&T)	http://www.arl.mil/
Carnegie Mellon University	Founder of CERT for Internet; Provides advisories and tools	gowens@arl.mil http://www.cert.org/ http://www.cmu.edu/
CSRC - Computer Security Resource Clearinghouse	Collects and disseminates compusec information and assistance; encryption support and incident handling	http://www.csrc.ncsl.nist.gov/
Lawrence Livermore National Lab	Department of Energy focus in support for: Computer Incident Advisory Capability (CIAC); Computer Security Technical Center (CSTC); Department of Energy - Information Security (DOE-IS)	http://www.llnl.gov/ http://www.ciac.llnl.gov/ http://www.ciac.llnl.gov/cstc http://www.doe-is.llnl.gov/

TAB H-1

Lincoln National Lab	FFRDC specializing in advanced electronics, network survivability, air traffic control, and radar/space systems - USAF affiliation	http://www.ll.mit.edu/
NRL - Naval Research Lab	R&D for IW/EW/Sensing technology; Information Technology Division (Code 5300)	office@sst.ll.mit.edu
Rome Lab	USAF affiliated R&D for information systems: Info & Intelligence Exploitation; Information Grid; Information Technology Division	http://www.nrl.navy.mil/
Sandia National Lab	R&D focus for computers, information science, pulsed power, SCADA assessments	http://www.sandia.gov/
SPAWAR / IOCOF	Develop, procure, field and support interoperable Navy IW systems (PD16); IOCOF - Information Operations Center of the Future: Provides integrated IO strategies, concepts, and services; assesses technologies; experimentation; and wargaming	http://www.spawar.navy.mil/ http://www.infosec.navy.mil/code72.html
		IOCOF web site under revision

Selected Computer Emergency Response Teams Worldwide

Response Team	Constituency	E-Mail/WWW URL
Advanced Network Services, INC (ANS)	ANS Customers	Ans-cert@and.net http://www.ans.net
Air Force CERT (AFCERT)	Air Force	Afcert@afcert.csap.af.mil
Apple Computer	Apple Computer	Isefton@apple.com
Australian CERT (AUSCERT)	Australia	Ausc-cert@auscert.org.au Http://www.auscert.org.au
Bellcore	Bellcore	Sb3@cc.bellcore.com
Boeing CERT (BCERT)	Boeing	Compsec@maple.a1.boeing.com
BSI/GISA	German Government	Fwf@bsi.de http://www.cert.dfn.de/eng
CCTA	UK Government and Agencies	Cbaxter.esb.ccta@gnet.gov.uk
CERT Coordination Center	UNIX, Internet Research	Cert@cert.org http://www.cert.org
CERT-IT	Italian Internet Sites	Cert-it@dsi.unimi.it
CERT-NL	SURFnet Sites	Cert-nl@surfnet.nl http://www.nic.surfnet.nl/surfnet.security.cert-nl.html
Cisco Systems	Cisco Systems	Karyn@cisco.com

TAB H-1

Response Team	Constituency	E-Mail/WWW URL
DEC SSRT	Digital Equipment Corp and Customers	Rich.boren@cxo.mts.dec.com
Defense Research Agency Malvern	Defense Research Agency	Shore@ajax.dra.hmg.gb
DFN CERT	Germany	Dfncert@cert.dfn.de
DISA	MILNET	Sec@cc.ims.dsa.mil
DoD ASSIST	DoD Interest Systems	Assist@assist.mil
DOE CIAC	Department of Energy	Ciac@llnl.gov http://ciac.llnl.gov
DOW USA	DOW	Whstewart@dow.com
EDS	EDS and Customers	Jcutle01@novell.trts01.eds.com
FedCIRC	Federal Gov/Civil Agencies; Incident reports & handling	http://www.fedcirc.gov/ fedcirc@fedcirc.gov
FIRST	Forum of Incident Response and Security Teams	First-sec@first.org http://www.csrc.ncsl.nist.gov/first/
General Electric	GE Businesses	Sandstrom@gies.ges.com
Goddard Space Flight Center	Goddard SPC	Hmiddleton@gscmai.nasa.gov
Goldman, Sachs and Company	Goldman, Sachs offices Worldwide	Safdas@gscsco.com
Hewlett Packard	All HP-UX Customers	Security-alert@hp.com
Israeli Academic Network	Israeli University users	Cert-1@vm.tau.ac.il
Janet Cert	All JANET networks	Cert@cert.ja.net

Response Team	Constituency	E-Mail/WWW URL
JP Morgan	JP Morgan employees and consultants	
MCI	Corporate Systems Security	6722867@mcimail.com
Micro-BIT Virus Center	Anyone	Ry15@uni-karlsruhe.de
Motorola CERT	Motorola	Mcert@mot.com
NASA (Ames Research Center)	Ames Research Center	Hwater@nas.nasa.gov
NASIRC - NASA Automated Incident Response Cap.	NASA and International Aerospace Community	Nasire@nasirc.nasa.gov http://nasirc.nasa.gov/NASIRC_HOME.html
NavCIRT	U.S. Navy	naveirt@fiwc.navy.mil http://infosec.nosc.mil/naveirt.html
NIST/SCRC	National Institute of Standards And Tech.	jwack@nist.gov http://cs-www.ncsl.nist.gov
NORDUnet	NORDUnet	Ber@sunet.se
Northwestern University	Northwestern Faculty/Staff/Students	r-safian@nwu.edu http://grumpy.asns.nwu.edu/nu-cert
Penn State University	Penn State Faculty/Staff /Students	Krk5@psu.edu
Purdue CERT	Purdue University	Pcert@cs.purdue.edu http://www.cs.purdue.edu/pcert/pcert.html
Renater	Minister of Research and Education	Morel@urec.fr

TAB H-1

Response Team	Constituency	E-Mail/WWW URL
SBACERT	Small Business Nationwide (US)	Hfb@oirm.sba.gov
Silicon Graphics, Inc	Silicon Graphics User Community	Security-alert@sgi.com
Stanford University NST	Stanford University Faculty/Staff/Students	Security@stanford.edu http://www.stanford.edu/security/
SUN Microsystems	SUN Customers	Mark.graff@sun.com
SWITCH	Swiss Universities and Government	Cert-staff@switch.ch http://www.switch.ch/switch/cert
TRW Inc.	TRW Network and System Administrators	Zorn@gumby.sp.trw.com
U.S. Sprint	SprintNet(X.25) and Sprint Link (TCP/IP)	Steve.mathews@sprint.sprint.com
UCERT	UNISYS Users	Garb@po3.bb.unisys.com
Veterans Health Administration IRT	Veteran's Health Administration	Frank.marino@forum.va.gov http://www.va.gov
Westinghouse Electric Corp.	Westinghouse Corp	Nicholson.m%wec@dialcom.lymnet.com

TERMS OF REFERENCE



ACQUISITION AND
TECHNOLOGY

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

FEB 29 2000

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board Task Force on Defensive Information Operations

You are requested to form a Defense Science Board (DSB) Task Force to review and evaluate DoD's ability to provide information assurance to carry out Joint Vision 2010 in the face of information warfare attack.

Tasks to be accomplished:

Using the "1996 DSB report on Information Warfare – Defense" as the departure point, address the following:

- What is the status of action on the recommendations?
- Where there are shortfalls, what are the barriers to action and what should be done?
- What important aspects did the 1996 Task Force miss that should have been addressed?
- Assess the recommendations of other important reports that have addressed information assurance issues.

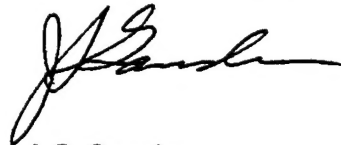
The Defensive Information Operations Task Force will determine:

- Adequacy of the process toward the information assurance goals needed to carry out Joint Vision 2010.
- Adequacy of the Department's readiness to project and sustain power in the face of information warfare attacks.
- The appropriate role(s) and capability of DoD to provide information assurance in support of Homeland Defense and in support of Critical Infrastructure Protection.
- Recommendations for research and development which are uniquely in DoD's interest, and thus not likely to be accomplished by the private sector in the time required to meet DoD's Defensive Information Operations objectives.
- Areas in which DoD should seek strong partnering relationships outside DoD, such as with the Critical Infrastructure Assurance Office (CIAO).
- The Task Force should provide an interim report by June 30, 2000 and the final report around October 2000.



The study will be co-sponsored by the Under Secretary of Defense (Acquisition, Technology and Logistics) and Assistant Secretary of Defense for C3I. Mr. Larry Wright will serve as the Task Force Chairman; Col Gregory Frick will serve as the Executive Secretary; and Maj Tony Yang, USAF, will serve as the Defense Science Board Secretariat Representative.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5104.5, "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, United States Code, nor will it cause any member to be placed in the position of acting as a procurement official.

A handwritten signature in black ink, appearing to read 'J. S. Gansler', with a stylized, flowing script.

J. S. Gansler